Tow Center for
Digital Journalism
A Tow/Knight Report

The Rise of the Security Champion: Beta-Testing Newsroom Security Cultures

Jennifer R. Henrichsen

Columbia Journalism School

Funded by the John S. and James L. Knight Foundation.

Table of Contents

Executive Summary

A number of factors contribute to the development of information security cultures in the newsroom, including investment in information security specialists who liaise with journalists about their specific needs and provide both informal and formal security training. Or news organizations may hire individuals in traditional roles, such as part of the IT department, but who also have information security knowledge. Journalists also bring information security knowledge into the newsroom out of curiosity, and the belief that information security practices are important for them to get stories and do their jobs. These security champions—who become trainers by accident—work to support colleagues and convince them of the need to adopt more secure practices, through informal conversations, brown-bag lunches, and training sessions at the individual, desk, and newsroom level.

Despite these developments, information security cultures in many newsrooms are nascent for reasons including ongoing financial crises and labor precarity in journalism, both of which can limit the allocation of resources for information security. Moreover, journalists dislike taking security steps that might slow down their reporting in jobs that are already precarious, and awareness of the

myriad security risks to journalists and news organizations is limited. All of these problems may be compounded by a lack of institutional buy-in and provision of resources to deal with these risks; often, silos between different parts of a news organization impede information sharing about security internally and externally to the newsroom; and institutional memory related to security may suffer when a trainer leaves. Newsrooms are organizations which, depending on size, financial state, ethos, and management structure, may suffer from both bureaucratic inertia and traditional power structures that limit change. But smaller organizations with less bureaucracy tend to have fewer resources to implement security related practices and policies. There appears to be more awareness of security practices in locations where news organizations are highly concentrated, such as the Acela corridor, rather than in more geographically distant locations elsewhere across the country.

Some journalists are "security champions" within their news organization, but between security considerations and journalistic craft, tensions may emerge: visibility, verification, usability, and speed. For example, journalists may try to protect themselves from online harassment by limiting communication channels such as direct messages (DMs) on Twitter, yet by doing so, they also reduce the number of ways that potential sources can communicate with them. In the last two

years, more news organizations have adopted the anonymous whistleblowing platform SecureDrop, but because of its anonymous nature, it can be challenging for journalists to verify the information received with it. Additionally, secure technologies like PGP encryption for email are challenging for many journalists and sources to use, which limits the adoption of the tool by both parties. Secure communications may also slow down publication, and speed is a currency that journalists and editors prize and prioritize. Journalists may prioritize a source's comfort with regard to communication, so if sources do not push for encrypted communications then journalists won't necessarily do so either. Among some journalists there is a resistance to the notion of protecting a source because it belies a so-called bias and lack of objectivity. However, in some cases, such as in the investigative realm, journalists are motivated to learn information security technologies to protect their sources, while for others, taking steps to improve information security operates as a signaling mechanism to future sources to say that they can be trusted with the source's story. Sometimes it is less about source protection and more about concerns that the credibility of the news organization may be at risk if internal communications about a story are leaked or subpoenaed.

Security, although networked in nature, is not always viewed as a collective issue or one requiring a collective response. Depending on their role in the news

organization and their knowledge about information security, journalists and management may not believe certain secure practices are necessary or applicable to them. Additionally, some journalists have a "security by obscurity" mental model which limits their willingness to implement information security technologies because they believe that, since they are not working on anything "sensitive," they have little to no risk of digital attacks. Older, more established journalists may not see why certain new technologies are necessary to journalistic and editorial workflows. The dynamic and yet precarious nature of journalism also encourages journalists to use their personal accounts and devices and various wi-fi connections as they travel and research a story, despite heightened insecurity.

Further, journalists may not take the time to threat model or develop and follow a risk assessment. They may not be up to date because of how quickly secure technologies change and how frequently vulnerabilities arise. Such varying information can result in a form of security nihilism, in which journalists give up trying to use security technologies because of the caveats and complexities of such practices. Depending on the resources available to them, they might not have individuals to reach out to for expertise on the tools and practices, and may stick with known practices and habits. Shared norms around which platforms to use (e.g.

Slack) can contribute to increased vulnerabilities if they are used without understanding the ways in which information is transmitted or stored.

Journalists may be hesitant to share their practices or knowledge about information security because they may have a sense of bravado or competition, or are concerned that doing so may make them more vulnerable to security risks. The power dynamics between editors and journalists, and journalists and sources, may encourage less secure practices in order to obtain a story and get it out quickly. Responses to perceived or real restrictions on journalists' autonomy may result in resistance, reluctance or circumvention of security practices. Security practices also tend to be reactive, following a concerning incident, rather than proactive, which can limit their effectiveness.

Security concerns overlap with other dimensions of journalistic practice including legal concerns related to information protection and subpoena requests. Information security practices necessarily engage with existing networks and infrastructures that have insecurities and vulnerabilities, while new vulnerabilities can be introduced when the integration of systems and tools is necessary but not supported. Sometimes security trainers and IT staff try to forefront security without understanding the particular needs of journalists and their workflow, which in turn

can result in journalists circumventing restrictions in order to pursue and publish their story.

A number of elements are necessary to facilitate the development of information security cultures in newsrooms. These include:

- Increased literacy around information management and security throughout the newsroom; policies and practices at the organizational and individual level, beginning with onboarding of new staff in the organization
- A shift in perceptions of what information security practices can provide to journalism (including empowerment of sources) and an understanding of how they are needed
- Ongoing training sessions to encourage sustained behavior change; development of secure and usable technologies to facilitate widespread adoption from sources to journalists
- Buy-in and a cultural expectation that security is important from the management and editorial level
- An understanding that developing an information security culture is ongoing, iterative, and proactive, and needs to be integrated into existing journalistic norms and workflows

Introduction

Journalists have long considered the United States a country that upholds the right to report critically and independently. Yet, an increase in government-led leak investigations, online harassment and physical attacks against members of the media has begun to puncture what was a robust environment for freedom of the press in the United States. Contributing to this deteriorating environment is the current US President, Donald J. Trump, whose constant attacks on the press have aimed to delegitimize the media and their role in holding power to account. Trump has called the media the "Enemy of the People" and has leveled false accusations against them near-daily in an effort to persuade citizens to disbelieve negative media reports about him.[1] Such an environment reduces trust in the media among members of the public and increases cynicism and passivity.

The current administration's demonization of the media has also contributed to an uptick in online and offline harassment and physical violence against its members. The president's rhetoric stirs up rage at his trademark rallies, where he encourages his supporters to hassle and assault reporters.[2] Some of his supporters

[1] https://cpj.org/blog/2019/01/trump-twitter-press-fake-news-enemy-people.php
[2] https://qz.com/1345622/video-of-a-trump-rally-crowd-harassing-the-press-in-tampa/; https://www.washingtonpost.com/blogs/plum-line/wp/2018/10/19/trump-encourages-violence-ag

have sent death threats; some have plotted to murder members of the media.[3] Although press freedom organizations have long tracked physical violence, imprisonment and assault among journalists around the globe, it has only been in recent years that press freedom groups have turned their attention to the United States.[4] Since its establishment in 2017, the US Press Freedom Tracker has documented more than 400 incidents involving press freedom violations.[5] Physical attacks include journalists who face violence and injury or equipment damage in the course of their work or from a targeted attack. Reporters have been attacked at Trump rallies, assaulted during live broadcasts, punched in the face and called purveyors of "fake news," and harassed and manhandled when covering protests—to name but a few instances. The physical attacks and online harassment are taking their toll on journalists, resulting in mental health crises and burnout.[6]

Additionally, there has been intensifying online harassment against journalists in the US and abroad. According to a 2019 survey by the Committee to Protect Journalists, online harassment was identified as the biggest safety issue for

---

ainst-reporters-and-his-supporters-cheer/; https://www.newsweek.com/trump-supporter-arrested-assault-journalist-rally-1444834

[3] https://www.axios.com/violence-against-media-bombs-shootings-trump-a59584cb-ac2c-4813-bfef-7b3a4233690d.html

[4] https://cpj.org/2017/08/new-website-to-track-press-freedom-violations-in-u.php

[5] https://pressfreedomtracker.us/blog/3-years-tracking-our-january-2020-newsletter/

[6] https://cpj.org/blog/2019/09/canada-usa-female-journalist-safety-online-harassment-survey.php

journalists.[7] Indeed, 90% of respondents in the US (out of 115 surveyed) believed it was the biggest threat. Eighty-five percent of respondents agreed that journalists have become less safe in the last five years. More than 70% said they had experienced safety issues and threats with the majority related to verbal harassment followed by online harassment. Female journalists are more likely to experience digital sex-based discrimination than their male peers[8] and minority journalists. Those who cover hot-button issues like white nationalism or race are often targeted.[9]

Journalists also have experienced a wide range of threats from phishing (messages containing malicious links) and distributed denial of service attacks (which take a website offline) to software and hardware exploits of a user's devices, among other hacking attempts.[10] In 2014, Google experts discovered that 21 of the world's 25 most popular media outlets were targets of state-sponsored hacking attempts.[11] In 2013, the Chinese government hacked *The New York Times*,

---

[7] https://cpj.org/blog/2019/09/canada-usa-female-journalist-safety-online-harassment-survey.php
[8] https://www.cjr.org/the_media_today/female-journalists-harassed-twitter.php; https://www.cjr.org/special_report/reporting-female-harassment-journalism.php; https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf; https://www.womensmediacenter.com/speech-project/research-statistics; https://unesdoc.unesco.org/ark:/48223/pf0000232358
[9] https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf; https://www.osce.org/fom/220411?download=true; https://cpj.org/2018/11/digital-safety-protecting-against-online-harassmen.php
[10] https://unesdoc.unesco.org/ark:/48223/pf0000232358
[11] https://www.cnet.com/news/watch-out-journalists-hackers-are-after-you-google-says/

the *Washington Post* and the *Wall Street Journal*[12], and the Syrian Electronic Army hacked the Associated Press, resulting in a tweet that briefly sent stocks into a nosedive.[13] More recently, the *Times*'s Moscow Bureau was targeted by Russian hackers.[14]

Another concern facing journalists is the increasing ubiquity and interconnection of digital technologies, which can generate data and metadata about ourselves, our networks, our locations, and our habits. Of course, there are numerous positive aspects of digital technologies for journalists; but they also track and collect data, which can compromise key tenets of journalistic practice such as communicating with sources. Journalists, as collectors, curators and disseminators of information, are at heightened risk for potential observation and investigation by powerful entities they hope to hold to account. The Snowden revelations clarified our understanding of the nature of some surveillance programs

---

12 https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html; https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

13 https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

14 https://www.nytimes.com/2016/08/24/technology/new-york-timess-moscow-bureau-was-targeted-by-hackers.html

that can implicate journalists and journalism, and we need only look to the news to see other examples of journalists being surveilled, their communications accessed, or their sources investigated.

Although thinking about information security technologies may be particularly relevant for our current administration, there were also intensifying efforts to investigate the sources of leaks during the Obama Administration. Indeed, the Obama Administration's Justice Department prosecuted more than twice as many leakers under the Espionage Act than in all previous administrations combined. In 2013, law enforcement secretly obtained the records for more than 20 telephone lines associated with AP journalists, including their home phones and cell phones, ostensibly to identify the source or sources behind a specific story.[15] Meanwhile the FBI sought and obtained a warrant to seize all of former Fox News reporter James Rosen's potential communications with his source, including his personal email, phone records and his security badge records to identify his movements to and from the State Department.[16] [17]

---

15 https://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html

16 https://www.washingtonpost.com/local/justice-departments-scrutiny-of-fox-news-reporter-james-rosen-in-leak-case-draws-fire/2013/05/20/c6289eba-c162-11e2-8bd8-2788030e6b44_story.html

17 https://www.cjr.org/watchdog/daniel-hale-intercept-leakers.php

Surveillance has gained new power and relevance in the last several decades as the creation and deployment of new technologies expanded the capacity to surveil and be surveilled. Surveillance—in its myriad forms—is intricately intertwined into our daily practices and experiences living in a digitally connected society. Journalists, as collectors, curators and disseminators of information, are uniquely positioned to be at risk from routine and automated monitoring, as well as from sophisticated and targeted surveillance by powerful corporations and states.

Thus, journalists and their sources are unable to know how or to what extent they may be monitored, or how this information may be used against them.[18] Metadata trails can identify journalists and their sources without the threat of a subpoena, while the development of identification and surveillance software from facial recognition technologies at public venues to license plate scanning and CCTVs can exacerbate the problem.[19]

The use of spyware against journalists is increasing in many countries around the world as states strive to control information and as technologies to surveil civilians become more sophisticated and inexpensive. This confluence of

[18] https://www.dni.gov/files/documents/RG/Effect%20of%20mass%20surveillance%20on%20journalism.pdf

[19] Bradshaw, Paul. (2017). "Chilling effect: Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations." *Digital Journalism* 5 (3): 334–352.

factors is creating a new reality for journalists globally as they seek to express their ideas online. The creation, sale, and deployment of surveillance technologies such as spyware suites have been increasing over the past several years, as indicated by leaked documents from the Wikileaks Spy Files, Citizen Lab investigations, NGO reports, and news articles. Recent headlines have shown sophisticated surveillance technologies being used to surveil Ethiopian, Bahraini, and United Arab Emirates activists, Saudi dissidents, Mexican and South American journalists and lawyers among others.[20] In January 2020, it was also revealed that *NYT* journalist Ben Hubbard was targeted by NSO spyware in June 2018.[21] The creation and selling of sophisticated surveillance systems by companies in western democracies to authoritarian regimes further facilitate this asymmetrical power dynamic between states and their citizens.

Adding to journalism's long list of challenges is the ongoing financial hardship and labor precarity facing most forms of media. Local news has been hit especially hard in the United States, with vast news deserts sweeping across the

---

[20] https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/; https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/; https://www.wired.com/story/evidence-that-ethiopia-is-spying-on-journalists-shows-commercial-spyware-is-out-of-control/; https://securitywithoutborders.org/resources/targeted-surveillance-reports.html

[21] https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/

States, contributing to ill-informed publics and severed communities. Meanwhile, nearly everyone from local and national print media to digital-first publications like BuzzFeed and Vice are laying off journalists in droves, reducing the ability of news organizations to take the pulse of current events, engage in investigative journalism, or inform the public and hold power to account. Nearly 8000 journalists lost their jobs in 2019, the highest level of attrition since the recession in 2009.[22] In response, news organizations are increasingly turning to syndicated content from wire services and other publications to fill in the holes in their local and city papers, while aggregator sites like Google News and Business Insider amass readers. Media companies are still struggling to find a successful business model for digital news, since digital advertising revenue sells for a fraction of the cost of ads in print publications in the past.

Despite these myriad and interconnected challenges, news organizations are only beginning to develop information security cultures in the newsroom. In this report, I examine how security cultures are being established and maintained in leading news organizations in the United States and the various challenges they face. I clarify how information security practices among journalists and in

---

22 https://www.businessinsider.com/2019-media-layoffs-job-cuts-at-buzzfeed-huffpost-vice-details-2019-2

newsrooms more generally may be changing journalistic cultures and norms of professionalism at a time of increased labor precarity and loss of trust in the media. In doing so, I connect the empirical study of journalists' changing digital news practices and newsroom culture to the larger question of what is and what journalism can be in an age of surveillance. Studying this issue matters because journalists are rhetorically instrumentalized as an essential component of a liberal democracy in their roles to inform the public and to be a check on powerful interests by reporting on corruption and malfeasance.

Method

Between February and December 2019, I conducted 30 semi-structured interviews with journalists, information security technologists, and media lawyers from national and local news organizations in the United States, and individuals from nonprofit organizations and academic institutions. I selected the subjects via a snowball sample (in which I began with a small population of known individuals and then expanded the sample by asking my interviewees for suggestions of others to interview) because of the sensitivity of the topics discussed. Interviewees represented a wide variety of organizations in terms of sizes and cultures, including small, medium and large organizations and mainstream, local, digital first and

investigative outlets. The aim was to obtain a diverse sample that reflected a range of perspectives and practices among journalists and adjacent actors in the newsroom. I also interviewed individuals associated with nonprofit news organizations and academic institutions, including OpenNews, Freedom of the Press Foundation and the New School because of the interviewees' experiences with information security or systems thinking at the organizational level. (See Appendix I for interviewee information.) The interviews were conducted in person, via phone or voice over Internet Protocol (VoIP). The interviews lasted an average of 46 minutes, and the interviews were recorded and transcribed.[23] I utilized Charmaz's (2006) constructivist grounded theory approach and open coding techniques on my collected data.[24] I also used a constant comparative method in which categories develop through an ongoing process of comparing units of data with each other.[25]

[23] In a couple cases the interview could not be recorded and therefore was not transcribed, but notes were taken.
[24] Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: Sage Publications.
[25] Lindlof, T., & Taylor, B. (2011). *Qualitative communication research methods (third edition)*. Thousand Oaks, CA: Sage Publications.

Caveats and Limitations

This report is written with an underlying assumption that journalism, in its capacity to inform and to hold power to account, is important for a democratic society and that communications between journalists, sources and editors are necessary for fulsome reporting on issues of import. This report relied on a purposive snowball sampling method because conversations about information security practices among journalists and newsrooms require trust. Therefore, it provides a snapshot of the different types of security cultures in newsrooms, which is not quantifiably generalizable, but has implications for other newsrooms in the United States. Additionally, this report will not identify any individual who has asked to remain anonymous.

Discussion and Findings

This section will examine three main components of the report. The first section will evaluate specific flashpoints that have raised security awareness among journalists. The second part will interrogate how security cultures are being developed in newsrooms and the third section will describe the different countervailing tensions limiting the development of security cultures.

1. Flashpoints Raising Security Awareness

Critical incidents raise awareness of information security for a time and can act as a motivator. Journalists indicated that current events and news stories related to the Snowden revelations, the DNC hack and Trump's election and ongoing data breaches are all contributing to a sense of information insecurity and awareness of a deteriorating environment. Additionally, certain incidents are hitting even closer to home and affecting journalists and/or their colleagues in personal and

professional ways. Journalists acknowledged the intensification of doxxing and online harassment, source exposure and legal threats, digital attacks from DDoS to hacking as reasons behind why they are starting to be more concerned about the information landscape and the vulnerabilities it poses to journalists and their ability to carry out their work. Additionally, journalists and information security technologists pointed to social and cultural shifts that are disabusing journalists of the notion that they are in a protected and venerable professional class.

The Snowden revelations and the Snowden story

The Edward Snowden revelations that began in 2013 ushered in a new understanding for many journalists about the capabilities of states and corporations to conduct widespread mass surveillance. News organizations who were able to report on the revelations with first-hand documents took immediate, extensive measures to try to ensure the classified documents they were writing about and the stories which resulted from them were secured before they were published and that they were able to report on the stories without being preemptively stopped. These measures varied in terms of technological sophistication and more analog measures.

The revelations of surveillance also spurred discussions among the journalistic community and the information security community about how to keep

one's communications private from prying eyes. Suddenly, there was significant interest among many in understanding how to encrypt communications in transit and how to encrypt your data at rest. Numerous digital security workshops sprung up and crypto parties were offered in cities around the world, seemingly at a greater pace and breadth than pre-Snowden. Said one national security journalist: "It took Snowden to make me really see in provable documented ways just how extensive the surveillance dragnets are. I had thought that I was utilizing secure measures of communications before and then it turned out…no. Really, this thing is hard to evade and you have to be extremely careful considering not just the technological capabilities of the dragnets, but the legal authorities that they claim in order to operate them and the application of them against citizens." (Interview, P7, April 19, 2019) Another reporter said that he quickly became interested in information security technologies after he joined *The Guardian* toward the end of the Snowden investigation because he knew that Snowden had required the recipients of information to install PGP, among other measures, but also because he saw his new colleagues at *The Guardian* "being very, very careful" and following protocols to protect the information. "Obviously that story was such a huge success that it really drove home to me how important that sort of thing was going to be for these kinds of stories from then on." (Interview, P1, March 25,

2019, p. 2) A data journalist who didn't work on the story nonetheless agreed and said how journalists were communicating with Snowden to get that story "was eye-opening to a lot of journalists." (Interview, P10, June 17, 2019, p. 12) A media lawyer said, "I think Snowden was a shot in the arm about awareness" both in terms of "what his documents showed, and also how the reporters went about doing that story." (Interview, P3, March 29, 2019, p. 5) Another journalist and digital security trainer said that all the workshops he did about information security at NICAR were jam-packed following the Snowden revelations and that "people still demand that topic at that conference." (Interview, P17, July 12, 2019, p. 1)

The Snowden story has been helpful in teaching journalists about information security. Said one security expert, "people are really drawn to the sexy stuff…when I'm giving trainings and we get into…all right, well, Edward Snowden just contacted you. Like what do you do next? Like people want to talk about that and people don't want to talk about why I think you shouldn't have your family on LinkedIn." (Interview, P6, April 9, 2019, p. 7)

DNC hacks and Trump's election

While the Snowden revelations opened up journalists' eyes to surveillance and ways to encrypt information, the Democratic National Committee (DNC) hacks brought home how easy and how devastating it is to be hacked. According to

a national security reporter, interest in information security among media professionals "definitely peaked again" following the DNC hacks. He said he thought this was:

> …partly because we all saw how relatively straightforward the hack was to start with, the phishing emails that were sent to people like Podesta…we've all seen emails like that in our inboxes…and just the huge damage and impact that could result from a…thoughtless click on one of these phishing emails… if these sorts of hackers want to target political groups, they probably are going to want to target media as well and they're going to want to try and discredit media who are reporting on them, and that we and other media organizations could definitely be a potential target for similar things. (Interview, P1, March 25, 2019, p. 3)

According to a data journalist, the DNC hack was a wakeup call for journalists because even though it was simple, it was sophisticated. "It's no longer the guy from Nigeria asking you for $5 million. That's not what they're doing anymore. It's much more sophisticated than that." (Interview, P10, June 17, 2019, p.11) Another journalist said that the DNC hacks should provide motivation to newsrooms to implement information security practices:

> Have them recall what Russia did with the emails that they hacked from the DNC and then later from John Podesta. What they did was to weaken them institutionally—they published the most embarrassing, the most cringe worthy, and the most internally divisive things they could. Unless you make this [information security] your priority, it's a matter of time before that happens to you. (Interview, P7, April 19, 2019)

Concerns about information security among journalists were also heightened leading up to and following the election of US President Donald Trump. A security professional for a digital-first company at the time said he "might've surfed on a wave of paranoia post-Trump." He continued:

> In fact one of the big discussions that we had in our newsroom was to emphasize before we understood what was going to happen with the election, the idea that both administrations would be threats to press freedom in different ways—that we would have to have different struggles. But I think ultimately when Trump won, it was such an emotional response. (Interview, P6, April 9, 2019)

A media lawyer for an elite news organization said he saw an increase in the volume of threats that journalists faced during the 2016 US Presidential Campaign:

> "…There would be isolated incidents before that where a story would cause great displeasure and you could expect this onslaught. But I think starting with the campaign, we started seeing more of it, then after the election we certainly saw it as well, you know. But I would say 2016 with the beginning of what I thought of was a real ramp-up.
>
> (Interview, P3, March 29, 2019, p. 2)

These concerns manifested in more journalists and sources willing to download and use the encrypted messaging service Signal. A national security journalist said he saw an increase in the expectation that Signal would be used for communications from people he didn't know or expect would be interested in using it and that this expectation surged in November 2016. "I definitely remember a spike in using it after Trump's election and I mean immediately after…" (Interview, P7, April 19, 2019)

According to another journalist who became the de-facto information security trainer in her newsroom:

> "…the 2016 election was really a big wake-up call for a lot of people…we already had some folks who were using ProtonMail. We started pushing folks pretty heavily toward Signal. And then…after the new year, after the election, was when we really did, like a big sweep. We taught everyone how

> to use Signal and taught everyone how to use ProtonMail. And then the following year, in 2017, we implemented SecureDrop and did another round of security training…the election really galvanized a lot of journalists." (Interview, P29, December 4, 2019, p.1)

An Information Security Director for an investigative outlet agreed. He said that the election of Trump was a flashpoint for many journalists. "I think that when Trump got elected…everyone was like, 'Oh, fascism is almost here.'" (Interview, P20, November 5, 2019, p. 26) The worsening environment for journalists has resulted in journalists becoming more interested, but not necessarily eager to learn more about information security to protect oneself. An information security technologist said he saw an increase in journalists' interest in security because they were getting "snapped out of" their day-to-day by a president "who is attacking the press on the television, on Twitter, every single day." This "felt extremely jarring. It felt shocking, it felt unusual to reporters. And suddenly they're paying attention. And security is something that people feel that they have some control over…" (Interview, P25, November 20, 2019, p. 9)

Ongoing breaches

The increase in the number and scale of data breaches and scandals in recent years have also raised journalists' consciousness to the risks and repercussions of

insecure practices by companies, agencies and individuals. Said one cybersecurity reporter, the 2014 Sony hack[26] in particular was a "big catalyst" and "showed everyone that it could happen to anyone." (Interview, P19, October 29, 2019, p. 9) He continued, "I mean we're literally talking about a company that makes movies…no disrespect, but it's not the NSA, it's not the DNC. And they got all of their emails plastered on Wikileaks…it was a great case study for saying, 'Hey guys, this could literally be us next week. We need to take this seriously.'" (Interview, P19, October 29, 2019, p. 9)

Another shocking moment was the Cambridge Analytica scandal. "Since then we have been asking some more pointed questions in the media, but also as citizens, just about the nature of these tech companies. Like what kind of access do they have? Should they have that access? Under what circumstances should they have access to our personal data?…I see people asking themselves about alternatives more than ever" said an information security technologist. (Interview, P25, November 20, 2019, p. 11)

To others, it's been the ongoing nature of such breaches that have increased journalists' consciousness. Said another national security reporter, "The steady

26 https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

drumbeat of slightly scary infosec stories has just made people much more aware in general that their data is probably fragile and slightly precarious and that people shouldn't automatically assume it's secure." (Interview, P1, March 25, 2019, p. 4)

Intensifying harassment and doxing

Additionally, there have been intensifying online harassment and doxing campaigns against journalists.[27] According to a media lawyer at an elite news organization:

> "Domestically, there has been over the last two or three years, an increasing number of online threats, email threats, phone threats, usually targeting reporters who have for whatever reason made somebody unhappy, usually because of coverage of the Trump administration. Sometimes it's other topics, but it tends to be reflective of the partisan divide in the country today. And sometimes not directly Trump. It can be about perceptions of political correctness, about writing articles sympathetic about immigration or any of the other topics that tend to be hot-button ones." (Interview, P3, March 29, 2019 p. 1)

---

27 https://cpj.org/blog/2019/09/canada-usa-female-journalist-safety-online-harassment-survey.php

Journalists across a range of beats receive threats but female and minority journalists tend to be targeted more intensely and frequently. Additionally, journalists who cover local or national politics or extremism receive more sustained and severe abuse.[28] A journalist at a local media organization said her managers started to care more about doxxing[29] once the news organization diversified its staff a little bit. She said:

> "When I joined it was whiter than it is now. And this isn't a problem that white people face as much as brown and black people do…you hire a bunch of people and they start complaining about it so you're suddenly hearing more" about it. (Interview, P16, July 12, 2019)

She soon found that whenever she did a story, regardless of whether it had to do with race or diversity, she would receive harassing emails. "When I finally told [my editor] that we needed to do something about it was when I was doing stories that had nothing to do with any controversial topic really. But people would still find a way to connect it with something." (Interview, P16, July 12, 2019)

Contributing to the likelihood of online harassment and doxing is the availability of one's personal information online. "I had a hacker buddy

---

[28] https://cpj.org/blog/2019/09/canada-usa-female-journalist-safety-online-harassment-survey.php

[29] Doxing (or doxxing) is when someone publishes your personal information in an attempt to harass and intimidate you.

who…used some search service and found my parent's names, a property they had owned, you know, in like two minutes. And it's like it's creepy. You know? That's what I would like to avoid." (Interview, P4, April 3, 2019, p. 6)

A cybersecurity reporter said that doxing was "the most likely scenario for most journalists…because it's easy to do and all it takes is angering a source or somebody connected to the source. And the damage can be very high, especially in terms of stress, remediation in terms of like, maybe you have to worry about how you go home, what bus you take, what public venues you attend." (Interview, P19, October 29, 2019) He added that it has been "underestimated for a long time…because it seemed like it was something that gamers did against each other…maybe journalists thought they were off limits, that no one would dox them…Maybe we got cocky or we got over confident that no one cared about our lives. But we now know that that's not the case…and it seems like some journalist gets doxed or threatened to get doxed…almost every week…." (Interview, P19, October 29, 2019)

This reporter said that part of the reason that doxing appears to be intensifying is because it is "literally kids play" and it's challenging to know how to successfully counter it:

> …there's no app that saves you from doxing. It's something that you have to sort of worry about all the time and defend against all the time. And the only way to do that is by having someone that keeps up with how doxing works and what to do to prevent doxing. And also again, you need to train journalists…I guess, worry less about the NSA or Russia hacking your email and worry more about random people on the internet publishing your home address on Twitter. (Interview, P19, October 29, 2019)

Anyone can dox a reporter, and some journalists expressed concern that they could be a target of online harassment or doxing from upset sources. Said one reporter, "I've certainly pissed off sources and not necessarily even sources…but people in that world who I've been uncomfortable having pissed off." So far, he said, "I've been pranked, but not hacked." (Interview, P4, April 3, 2019)

Journalists have more awareness and concern about doxing because they've reported on it or know someone personally who has experienced it. (Interview, P16, July 12, 2019) An information security trainer agreed and said that the journalists she's worked with have been more proactive about security in response to concerns about being harassed or doxed, especially if they've heard stories from colleagues about what has happened to them. She said, "I'd say it's definitely a main concern journalists have, but most of the people I've talked to haven't actually

been doxxed. I think they just see the potential of it happening…and they're scared and they want to take the preventive steps to reducing this information…There is a smaller set of people that have been targeted that way who have been very vocal of, 'This happened to me and this is the impact it had,' and that's been enough to encourage other people to start looking at ways to reduce it." (Interview, P12, June 25, 2019, p. 14) She argued that it is important to be proactive rather than reactive when trying to minimize the potential for online harassment and doxing because "when it's in a reactive situation, there's not a whole lot you can do." (Interview, P12, June 25, 2019, p. 18)

DDoS, hacking and source exposure

Other times, journalists and news organizations begin to care more about information security when they are directly targeted by distributed denial of service attacks (DDoS) or nation-state hacking attempts. Said one journalist and news apps developer:

> A couple years ago…We pissed somebody off on the internet and our email system was hit by a denial-of-service and nobody's email worked. At that point, I think, at least at [our news organization] everybody started learning about secure alternative ways of communicating. People started to realize

that we are vulnerable to threats like anybody else. (Interview, P17, July 12, 2019, p. 2)

There have been non-targeted attacks against news organizations in the form of ransomware, but also targeted attacks by individuals and nation states who want to intimidate news organizations and find out information. According to one information security technologist, nation states and powerful individuals don't want to be written about so they hire people to dig into who is writing stories about them, and learn who they are and what their motivations are in order to compromise them in different ways and to discredit them. (Interview, P28, December 4, 2019, p. 10) Another information security technologist concurred. He said that nation state actors "like to have a leg up when it comes to understanding whether or not you're reporting on them, and if so, how? What do you know? Who are you talking to?" (Interview, P25, November 20, 2019, p. 8) "It's rare that you'll have a hacktivist…who's going to hack a news organization because they feel a certain way about a story or something. That's not what we normally see." (Interview, P28, December 4, 2019, p. 10)

Cases in which sources have been exposed, arrested or charged with espionage, have also resulted in raised awareness and concern among journalists about the need to learn and successfully implement information security

technologies. One security technologist said that his organization had sources who were charged with espionage, which was definitely a “flag” and a concern for journalists in the organization. (Interview, P20, November 5, 2019, p. 25) Another cybersecurity reporter said, “We don’t want to do that. We don’t want to be the next guy that exposes a source, who gets the source arrested.” (Interview, P19, October 29, 2019)

Another data journalist said, “All the other sources who’ve gotten burned by poor operational security I think may have had the effect of…Wow…they had all the things, and it still didn’t work. It’s even harder than some people were pitching it to be.” (Interview, P10, June 17, 2019, p. 12)

Meanwhile, media lawyers described that when the government launches a leak investigation, “They don't need to come to [the outlets being investigated]. They run into a variety of complications when they come to us and there's the optics of it and everything else. I think that they would prefer not to and if they don't need to, they don’t.” (Interview, P3, March 29, 2019, p. 4) Instead the investigations are more centered on looking at government employee’s own electronic footprints. Another media lawyer agreed, “They don't bother subpoenaing us anymore, and I think that's because of information security reasons. They can just go get the data elsewhere. They can subpoena it from third

party providers. They can capture it using technological methods if reporters don't protect themselves." (Interview, P2, March 27, 2019, p. 2-3)

Cultural shifts

These challenges are occurring amidst cultural shifts facing the news media. The public has a lack of literacy about the media's role, which is complicated by tensions of a 24/7 news cycle in which reporters operate as pundits and confuse facts and opinion. Some have argued that the rise of the always-on news cycle has led to more commentary, opinion, and speculation which has resulted in less distance between factual information and other forms of information. (Interview, P8, April 19, 2019, p. 12)

There is also a perception that the news media is more partisan than it has been in the recent past, which has led some members of the public to treat it less seriously or accurately. According to a former CEO of an investigative news outlet, "[Y]ou have the president of the United States referring to the top of the journalism pyramid, *The New York Times*, as 'the fake news failing *New York Times*.' There are people that regard what they see there, if they see it at all, or if someone tells them about it, to be suspect." (Interview, P5, April 3, 2019, p. 1)

Not only do segments of society view all media as partisan, but some view journalism as the enemy.

> "[T]he thing that is so screwy about the universe that we live in, apparently, is that there actually are a bunch of people who do mess with journalists just for kicks. And they hang out on 4Chan and Reddit and whatever and decide to mess with people. But then there's also this parallel universe of people who…want to tear down journalism because they make money off of having bitter partisan divides be the way that we operate in the world now. So there are a lot of different folks with motivating factors out there who love to see real journalists fall down." (Interview, P8, April 19, 2019, p. 11)

An information security technologist who has worked with journalists for years concurred and said that there are "actors who want to see the media destroyed…Some of them are centralized actors, some of them are decentralized actors." He argued that it was essential that news organizations understand that "some communications are not about the free exchange of ideas, but rather they're part of an attack against the media and they need to be seen as that. So when I talk about harassment of reporters, that's an example where for a lot of organizations, they're slow to realize the nature of what I think we call today—bad faith attacks." He said it's important that the media see these types of communications for what

they are and not treat them like good faith exchanges of ideas that warrant responses. (Interview, P6, April 9, 2019) He said some organizations were better at this than others. "…Without naming names…some organizations are quicker to understand this. I think ultimately local news actually struggles with this because it's unclear sometimes when you wade in. I mean, that's part of the challenge of these things. It's unclear to a lot of reporters when they wade into a thing that they don't realize is a thing." (Interview, P6, April 9, 2019, p. 4)

According to an information security technologist and former journalist, news organizations need to understand that they have a duty of care to protect their newsroom. Journalists are facing doxing and online abuse and other attacks and "the duty appears on the organization as far as I'm concerned to protect these folks," the technologist said. "Someone posted your address because they don't like what you said about Trump. Like that's real, right? And we're in a new day and age and you can't have *no* digital defenses. It's not just about, like, encrypting a message that some source gave you. There's other elements to this." (Interview, P28, December 4, 2019, p. 9)

These elements include helping ensure journalists are prepared to combat online harassment and doxing as well as other challenges. According to another information security technologist, news organizations are "rather comfortable"

with legal challenges in which a "very powerful organization threatens to sue and the news organization says 'bring it on.'" Yet, they tend to "wither" when it's an attack from "social media mobs" who use shaming tactics to call for the firing of an individual or something similar. He said that the media "throws in the towel immediately in the face of that, where it seems to stand up very strongly to authoritarian governments or legal threats." (Interview, P6, April 9, 2019, p. 2) He added, that:

> Ultimately people need to feel safe doing this kind of work. So we want to make sure…to create a resilient newsroom…where people feel empowered to go and do adversarial reporting because they know that where they sit in their desk is safe and they know that their management will have their back. (Interview, P6, April 9, 2019)

This is especially needed in an environment in which the public response to journalism and journalists is more violent and immediate than it was in the past. "In today's day and age, people feel like they can like, 'oh I didn't like that story. I'm not going to argue about the stats behind it or the quotes. I'm just going to go after you as a human being.' Right? The gloves are off. That's how the public feels." (Interview, P28, December 4, 2019, p. 9)

2. Developing Security Cultures in the Newsroom

News organizations are developing security cultures through a variety of mechanisms and practices including adopting SecureDrop, providing tip pages with various ways to communicate with journalists, building in-house information security teams, and having internal sessions dedicated to information security topics through brown-bag lunch meetings and peer-to-peer learning of information security tools. More than 65 major news organization globally, including news organizations in the United States such as *The New York Times*, the *Washington Post*, ProPublica, and The Intercept use SecureDrop.[30] SecureDrop is an open source whistleblower submission system that news organizations can install to anonymously and more safely receive tips from sources. For five years, nonprofit news organization The Freedom of the Press Foundation has led the development of SecureDrop and helped news organizations install it. A significant number of news organizations publicly launched SecureDrop in 2017. A number of news

[30] Freedom of the Press Foundation 2019 Impact Report, https://freedom.press/news/freedom-press-foundation-releases-its-2019-impact-report/

organizations adopted or reinstated SecureDrop in 2019 including NBC News, Australian Broadcasting Corporation, The Crime and Corruption Reporting Project, The Dallas Morning News, Slate, Süddeutsche Zeitung, ProPublica, Business Insider and others.

Although many news organizations have had tip pages on their website for years, some announced new tip pages with the announcement of their SecureDrop installations. These tips pages generally include ways to leak to the news organization via various means including encrypted applications like Signal and WhatsApp, SecureDrop, postal mail, among other methods. Freedom of the Press recently reviewed the websites of more than 80 top online news outlets[31] and found that email and postal mail are the main ways investigative reporting sites solicit news tips, but Signal and SecureDrop are nearly as common.

[31] The review included the sites for the 50 top newspapers identified in the Pew State of the News Media survey, as well as the subset of their "digital-native" outlets that engage in investigative reporting, and a small selection of additional notable journalistic outlets, including nonprofit newsrooms, non-newspaper legacy media companies, and wire services.

Outlet	Email	GPG	ProtonMail	Postal Mail	Phone	SMS	Signal	WhatsApp	SecureDrop
Atlanta Journal-Constitution	✔								
Arkansas Democrat-Gazette	✔			✔	✔				
azcentral									
Baltimore Sun	✔				✔				
Boston Globe	✔		✔	✔	✔				
Buffalo News	✔								
Chicago Tribune									
Houston Chronicle	✔			✔	✔				✔
Cincinnati Enquirer									
Cleveland Plain Dealer	✔								
Hartford Courant									
Dallas Morning News									
Denver Post	✔				✔	✔			
Columbus Dispatch									
El Nuevo Día									
Detroit Free Press									
Indianopolis Star									
Milwaukee Journal Sentinel	✔			✔	✔		✔	✔	✔
Kansas City Star					✔				
Los Angeles Times	✔	✔		✔			✔		
Mercury News	✔								
Mlive									
mySA									
Newsday	✔			✔	✔			✔	✔
NJ.com	✔	✔	✔	✔	✔	✔	✔		
NY Daily News					✔				
NY Post	✔				✔				
New York Times	✔	✔		✔			✔	✔	✔
Orange County Register									
Omaha World-Herald									
Oregon Live									
Orlando Sentinel									
Philadelphia Inquirer				✔			✔		
Virginian-Pilot									
Pittsburgh Post-Gazette									
Sacramento Bee	✔		✔	✔	✔	✔	✔	✔	
San Diego Union-Tribune									
Seattle Times	✔	✔		✔			✔		
SF Gate	✔	✔		✔	✔		✔		✔
Honolulu Star Advertiser	✔				✔				
Minnesota Star Tribune	✔			✔	✔		✔		
St Louis Post-Dispatch									
South Florida Sun Sentinel									
Chicago Sun Times									
Syracuse Post-Standard	✔				✔				
Tampa Bay Times	✔	✔		✔	✔		✔		
Twin Cities Pioneer Press									
USA Today				✔					✔
Washington Post	✔	✔		✔			✔	✔	✔
Wall Street Journal				✔			✔		✔
Insider	✔			✔	✔				
BuzzFeed News	✔	✔			✔		✔		✔
Eater	✔						✔		✔
Engadget									
Gizmodo	✔								
HuffPo	✔								✔
Politico							✔	✔	✔
Slate	✔			✔					✔
The Daily Beast	✔			✔			✔		✔
The Verge	✔			✔			✔		✔
Vox	✔	✔							✔
CNN	✔	✔	✔	✔			✔	✔	
NBC News				✔			✔	✔	✔
ABC News	✔			✔	✔		✔	✔	
CBS News	✔	✔		✔	✔		✔		✔
Fox News					✔				
NPR	✔			✔					✔
The New Yorker									
The New Republic				✔					
New York Magazine									
Bloomberg News				✔					✔
Rolling Stone	✔			✔			✔	✔	
Vanity Fair									
Vice (Motherboard)	✔	✔		✔			✔		✔
ProPublica	✔			✔			✔	✔	✔
The Intercept	✔			✔			✔		✔
The Appeal	✔								
Associated Press				✔			✔	✔	✔
Reuters	✔	✔		✔			✔	✔	✔
McClatchy (DC)				✔					✔
Axios									
The Guardian		✔		✔	✔		✔		✔
	Email	GPG	ProtonMail	Postal Mail	Phone	SMS	Signal	WhatsApp	SecureDrop
TOTAL	42	14	4	36	23	3	28	13	27
TOTAL %	51%	17%	5%	44%	28%	4%	34%	16%	33%

Figure X. Tip Pages Reviewed by Freedom of the Press

In-house information security teams

Although many news organizations have had dedicated, in-house expertise related to physical security for some time, some news organizations are developing roles for information security in their newsroom. According to publicly available LinkedIn data, news organizations range from having no one dedicated to information security on staff to having many roles in the newsroom with information security in their job description. News organizations differ in size and resources, with *The New York Times* a leader in both. Therefore, it is perhaps unsurprising that, out of eight news organizations examined, it had the highest number of individuals with "information security" as part of their official title.[32]

Title	Year Started in Current Role
Executive Director of Information Security	**2013**
Senior Director of Information Security	**2017**
Information Security Analyst	**2017**
Senior Information Security Analyst	**2018**

[32] This assessment was completed in September 2019 and thus does not reflect changes since that time. It relied on publicly available LinkedIn data and therefore does not reflect individuals who chose not to list their title and affiliation on LinkedIn. Additionally, individuals who do not have information security in their title may still engage in information security issues in a news organization.

Incident Response, Information Security	**2018**
Information Security Training Manager	**2019**
Information Security Analyst	**2019**
Information Security Trainer	**2019**
Senior Information Security Analyst	**2019**
Associate Information Security Analyst	**2019**
Chief Information Security Officer	**2019**

Figure X. Information Security Affiliated Positions

The rise of the "security champion"

The majority of news organizations do not have a dedicated team for information security. As such, information security lives in different places within the news organization and is often not standardized within or across news organizations. One journalist and former information security trainer said that "it ends up in a lot of weird places" from data teams to investigative, national security, politics and even a special project innovations lab. "It varies depending on medium, it varies depending on corporate ownership structure." (Interview, P29, December 4, 2019, p. 8)

Another journalist and digital security trainer said that awareness of security in a newsroom spreads as a result of "proximity to people who are already concerned," whether it is because a reporter got doxed, or the news organization's

website was taken offline because of a DDoS attack. These incidents spur internal discussion, which in turn spreads awareness of the different types of steps people can take to mitigate such concerns and threats. (Interview, P17, July 12, 2019, p. 8)

Cross-pollination of security knowledge occurs across the newsroom with journalists from different desks swapping information and knowledge. According to one digital security trainer, such sharing of expertise has occurred throughout their newsroom with the international team helping the investigations team to learn how to do bigger international stories, and the investigations team acting like the digital security experts to the rest of the company, while the desk covering the alt-right were the ones who best understood the harassment piece. (Interview, P6, April 9, 2019, p. 11)

A few digital security trainers pointed to the importance of the investigative teams for spurring discussions about information security. One trainer said this was because the investigative journalists "know people that have had stuff happen to them" and "they're kind of curious that way." (Interview, P18, October 16, 2019, p. 6) Another journalist recounted how the investigative team in his news organization helped to ensure others knew the basics of information security and also offered to be a resource for more specific questions and follow-up. Another trainer said that "…investigations is going to be more interested in information

security than style", which "is an area we're still trying to navigate and find a good way to work more closely with these teams to help them understand the need…" (Interview, P12, June 25, 2019, p. 7)

Other times, a news organization has hired people who have a lot of knowledge about information security, but it's not necessarily part of their job description to implement anything specific related to it. Instead, when security knowledge transfer happens, it's "sort of happenstance." (Interview, P2, March 27, 2019, p. 11) Indeed, journalists who may be more technical, like data journalists, are sometimes counted on to help out the newsroom in various ways, including by answering security questions from other reporters. A developer and journalist said that his hometown paper doesn't have anybody in the newsroom who's a security expert "but they do have people who do technical work…And so having been in that role, in that newsroom, I know what type of tech support questions you get. And sometimes it's because the printer doesn't work. But other times it's because they're working on a story and they want to be able to figure out how to do a particular type of analysis. And in other cases it's a security question." (Interview, P8, April 19, 2019, p. 4)

Other times, journalists who are more technically inclined get pulled into a bridge role within their news organization because resources are scarce and

technical abilities differ. This type of role is more common among journalists with technological skills than those in non-technical roles in part because certain projects they are involved with need “communication and collaborations across different teams within the newsroom and also across different departments within an organization.” (Interview, P8, April 19, 2019) There is “just tons and tons of peer-to-peer training, whether it's somebody at the desk next to you, like, "Yeah, I can show you how to do a pivot table. That's what you need for this story that you're working on." Or, like, "I can do a brown bag lunch that explains how to install Signal on your phone.” (Interview, P8, April 19, 2019, p. 7)

According to a data journalist: “I think at the root of anything that I've been able to change at [my news organization] so far, it's just because I've cared about it…Anything that I've done, I've just gone ahead and done it, and then asked for sign-off. Asked for forgiveness, not permission, kind of thing. Generally, my managers have been very welcoming to any ideas I've had as far as changes to the team. It's not that they didn't think it was important. It's that they didn't think of it, or they didn't have time to think of it. I guess it's just finding sneaky ways to integrate things like that.” (Interview, P14, July 2, 2019, p. 10)

The reliance on data journalists as the information security experts is problematic according to a security technologist, because they are not necessarily

the same thing. “I remember when I was at *The Times* as a data journalist, I was…harassing my editor…to get on a phone with people at Freedom of the Press to talk about SecureDrop…What I’d hear in response was that they didn’t understand why doing so was important…IT and data journalists are not information security experts. But in your average news org they're the closest thing. That's what people believe. But it's not the right shape to go through that hole. It's not correct mapping at all. But, you know, it's like the best they have right now.” (Interview, P28, December 4, 2019, p. 16)

Anyone in the newsroom can be a so-called “security champion” or “security advocate” if they are sensitive to the notion that information security is important for journalistic practice. One media lawyer said she has found security champions across her organization. She said, “Interestingly, they're not all necessarily national security reporters. One of them was a science reporter. There was another one who was a guy who did visual work. They know a lot about the subject matter, and they know a lot about the technology, and they just happen to be really into it and they encourage people to use it in a certain way. They are, in some ways, some of the best ambassadors. They get it. They know how to do it, and they can explain it to their peers.” (Interview, P2, March 27, 2019, p. 12)

Other times, a lawyer in a media organization may believe that information security is important for journalists to learn and use in their work. A media lawyer said, “My interest in information security is really more of an intellectual one than a practical one. I don't want to use any of these tools themselves, but I do understand conceptually why they're really, really important…I’ve done some training for the reporters. I'm like, ‘Here's basically what the risks look like and what some of your options are.’ I can't make anybody do anything. I can just provide information. I think it helps that they feel like, ‘Well, there's a lawyer who says this is something that's valuable and so we will take that seriously.’ Then it's up to them to look into it.” (Interview, P2, March 27, 2019, p. 12)

Information security trainers’ leveraging of “security champions”

One way digital security trainers are trying to level up security in the newsroom is by having one-to-one conversations with certain journalists—so-called “security advocates”—to get them onboard with the notion that security is important and then have them advocate for improved security practices to the rest of their team. “We need to find a couple people to buy into what we're doing on that specific desk before we can make real progress with that

team when they don't already have that culture of security-mindedness on their team." (Interview, P12, June 25, 2019, P. 7)

Doing so helps to "foster the culture to create a community that is passionate about and interested in and supportive of the work that you're doing" said Runa Sandvik. When she joined the *Times* in 2016, she was part of the larger security team, "but there was no one that was dedicated to the newsroom. And in the newsroom, some people knew that there was a team, but couldn't name anyone on it. Some people had no idea there was a security team at all. There were people that didn't get what I was there to do. Didn't understand my role." She said that through finding "security champions" or "people across the newsroom that understand the role, understand the work, are interested in security" she was able to understand what they needed, share information, and help them drive best practice across their desks, teams or projects." This point of entry allowed for other discussions and training sessions to occur, whether in the form of a brown bag lunch, sitting in on someone's weekly meeting, or teaming up with different departments, like legal, to talk about risks related to travel. (Interview, P23, November 11, 2019, p. 7)

Another digital security trainer said that security champions are behind the development of security cultures in several places because they eventually start talking to their bosses and their peers and get people started thinking about

security, but “their mileage varies based on, like, how receptive management is.” (Interview, P18, October 16, 2019, p. 6)

The IT Department can also shape the culture of security within a newsroom

Sometimes technology staff who are in charge of securing journalists’ devices or device provisioning become impromptu security champions, said a digital security trainer. In the course of their work they realize that they could take security a bit further and facilitate working securely in a more systematic way. (Interview, P18, October 16, 2019, p.6) In other cases, it’s “a software developer that's, like, really into [the] Snowden stuff, basically. And it's just like, ‘Hey, we should get SecureDrop, that would be really useful. We should be protecting our sources and stuff.’”(Interview, P18, October 16, 2019, p.6)

The digital security trainer said that it is not necessarily an entire department that would advocate for working more securely, but rather one or two people who are “just really into the idea” and “read a lot on the subject” and “have a certain amount of knowledge on it…And are like, ‘Hey, we should do this too.’” (Interview, P18, October 16, 2019, p. 6)

Another journalist said that “at [his news organization], we’ve finally started expanding our IT side, so we have a new IT Director who is very on top of...it’s

like security is front of mind for him. I mean, he's been great to work with." (Interview, P17, July 12, 2019, p. 1) Another security technologist said newsroom IT workers tend to know more about security than in the past. (Interview, P29, December 4, 2019, p. 16) A security consultant for a large news organization concurred and said that "some of the best security champions come from our IT team and our infrastructure site reliability engineers." He added that, in his experience, this was the same for organizations like the *Washington Post* and Vox. (Interview, P6, April 9, 2019, p. 11)

Sometimes IT contributes to a more robust security culture, not by being an overt and visible security champion, but by keeping technologies in-house and relying less on third-party platforms, which might comply with subpoenas. According to one media lawyer: "[Our organization] does a couple unique things to begin with. We don't use a lot of third party servers. Everything is an internal proprietary system. Part of that is because of the way our distribution network works. We needed to have our own system. There's a certain amount of security that's built into that…and I think there is a perception that it's adequate. I don't think the journalists feel like, for the most part, they need to do more than that." (Interview, P2, March 27, 2019, p. 11)

Journalists lean into their own networks for security knowledge

Other times, support for learning information security practices arises within a subcommunity, like the cybersecurity beat. According to one cybersecurity reporter, “I do think that [cyber]security journalists are relatively supportive of each other…because it's a hard subject to cover and…many of us end up meeting in the same handful of major conferences and frankly we talk to a lot of the same sources, that for whatever reason, it is a relatively nice camaraderie.” (Interview, P4, April 3, 2019, p. 4) He also added that there has “been a dramatic shift in how security practitioners and security experts address people who are not experts and that includes journalists.” He’s noticed that there has been “Way less condescension. Way less gatekeeping…I think they're more patient, kinder, have better rapport [with] journalists in general.” (Interview, P4, April 3, 2019, p. 4) This better rapport and communication can help to improve journalists’ knowledge of security and the implementation of information security tools and practices among readers. In turn, the cybersecurity reporter can spread knowledge about security internally in terms of what practices and devices journalists can use, but she may also serve as a translator for the rest of the newsroom when wide-scale hacking stories and data breaches occur. “Like the gist of the DNC hack wasn't that complicated but some of the specifics, it would be easy to get lost in the weeds and

you need to have...somebody on staff who can parse that quickly for the rest of the newsroom," said the cybersecurity reporter. "And so it's kind of a one, two strike of this person both has a [cybersecurity] beat, but also can be the larger translator for the rest of the newsroom." (Interview, P4, April 3, 2019, P. 5)

Another information security technologist described how journalists go within their own networks to understand security concerns and questions. "It's very insular. People go within their journalistic confines—their dim sums or coffees or whatever they do—and they share and trade information there. Sometimes at conferences, but usually it's pretty siloed, based on trust." (Interview, P28, December 4, 2019, p. 2) A security analyst also noted how journalists often rely on their own networks, including their one or two security people. She talked about how she wanted to encourage journalists to draw on the resources of her news organization's information security team and also "empower people to take security into their own hands" by showing them how to investigate and evaluate risks on their own. (Interview, P15, July 5, 2019, p. 15)

Sometimes the publication of a piece that explains how journalists used secure technologies to get the story can teach journalists reading or watching the piece to take similar precautions. (Interview, P28, December 4, 2019, p. 2) Additionally, journalists tend to become more concerned, aware, and interested

about information security issues when they read about them in the news or hear about them from their peers. In response, information security teams pivot to what's top of mind. Said one information security analyst, "A big thing that I like to focus on is travel security and what goes into that process…news cycles have brought this up really recently." (Interview, P15, July 5, 2019, p. 7)

Journalists also learn about information security from virtual peer networks like the News Nerdery Slack, which also has a security channel for individuals who work as journalists or have other roles in the newsroom to discuss questions and concerns. According to one interviewee, the News Nerdery Slack is a "consistent and ongoing space" for security conversations while other lists have "fizzled," but she also pointed to the need for newsrooms to utilize their own networks to better support security cultures. (Interview P9, April 22, 2019, p. 8)

Various efforts to encourage the diffusion of information security technologies and practices in newsrooms have involved outside groups who have utilized a peer-to-peer learning framework. In 2017, OpenNews and BuzzFeed's Open Lab created "The Field Guide to Security Training in the Newsroom," a modular curriculum for security trainers and "accidental experts" who are responding in non-formalized ways to requests from peers and others in the

newsroom about digital security and privacy questions.[33] The guide was a result of a community effort that was kickstarted in the summer of 2017 when a dozen journalists and experienced security trainers convened at Northwestern's Knight Lab to create the first draft of the guide, which was then subsequently tested and refined in the following months.

The goal of the guide was to provide a teaching resource to newsroom workers without the money to bring in outside experts. According to one of the leads on the project, "…we felt like the specific newsroom need was for support for people who kind of accidentally end up as trainers because they don't have necessarily a security background themselves, but they're the nerdiest person in the newsroom;" someone who fools around with technology all the time and is the person that folks go to for help. (Interview, P8, April 19, 2019, p. 2) The guide provides lesson plans that allow journalists to teach their peers about security tools and practices. "We wanted to hit that specific newsroom need of, like, 'We're a small newsroom. We do regional coverage. We don't have a security expert on staff. How can we kind of level up our people and do some peer training?'" (Interview, P8, April 19, 2019, p. 2-3) He said "a big point and goal of writing the guide was to identify and support a handful of meaningful steps that newsrooms

[33] The author of the report was involved in the creation of this guide.

could take to improve digital security."(Interview, P8, April 19, 2019) Each of the lesson plans represents a single concrete thing that an individual can do to incrementally improve security. (Interview, P9, April 22, 2019, p. 7)

Amanda Hickman, who helped lead the development of the guide, gathered feedback from individuals who used the guide to train others in their newsrooms. Participants in the sessions had a significant level of interest in understanding the specifics of technologies and how these technologies worked together. Many of the questions were about how something works or why something happens, as well as what Google has access to and whether Facebook is listening to one's audio. She said the questions reminded her of ones someone might have of a nutritionist, because they were very general questions that probably everyone wants the answer to. "For me, that kind of reflected the fact that I think there's a lot of frustration and confusion in general…people have a lot of questions about privacy and security and they don't feel confident about where to get reliable answers…People need safe places to ask stupid questions and they need the need that about everything. I think security is a place where a lot of people feel dumb and they feel like they are supposed to know and they don't want to acknowledge that they don't know…" (Interview, P9, April 22, 2019, p. 4-9)

Interviewees differed as to whether newsrooms need a specific position dedicated to teaching journalists about information security, or whether a more sustainable change would arise from reporters becoming more knowledgeable about information security and training others. According to Hickman, "…I think there's room for there to be somebody whose paid responsibility it is to be aware of risk and threats and concerns and take responsibility for keeping the rest of the newsroom up to date…" (Interview, P9, April 22, 2019, p. 8) Some information security trainers are wary of this approach because of the ease with which a news organization could let a position and the person go. (Interview, P28, December 4, 2019, p. 17)

There has also been movement from proprietary thinking around information security to more collaboration, with the rise of technologists in the newsroom, and technologists acting as intermediaries. According to one technologist, "…there was a hesitance to even share tools in the beginning or like processes that people use internally… 'this is how our newsroom collects these things, or how we handle that stuff.' There was an idea that needs to be a secret…but I think as more technologists get involved in news gathering, they share the idea that security through obscurity isn't a thing. (Interview, P28, December 4, 2019, p. 13) Despite this supposed opening-up of security practices, he acknowledged that journalists

are competitive and protective of their methods and sources because of the work that they've put into them. "…there's an element of 'I earned this,' you know?…maybe I don't want to tell you everything that's going on here because these are my sources." (Interview, P28, December 4, 2019, p. 13)

Toward a "culture of encouragement to be secured"

According to a journalist who worked on the Snowden story, an awareness and respect for security pervades his news organization even as it treats security needs for a story on a bespoke basis. He said, "…it's case by case and it's beat by beat really. But we're definitely a culture of encouragement to be secured, let's not use open email with sources that need confidentiality and let's always be aware of that stuff." (Interview, P1, March 25, 2019, p. 4)

Similarly, at *The Intercept*, journalists are largely comfortable with implementing information security practices and technologies. This is partly due to "a culture where people realize that security is important." (Interview, P20, November 5, 2019, p. 2). "People seem to be fine with that [information security] because they're like, "Well, it's *The Intercept*. We have to do it…I think once there's organizational support for doing all of this stuff, then it's actually not that bad. Even using PGP, which is awful. But it's not that bad if somebody else sets it up on your computer." (Interview, P20, November 5, 2019, p. 7)

Additionally, at other news organizations, like *The Daily Beast*, a climate of security has started from the top. According to a journalist who used to work there: "Our editor-in-chief came from *Wired,* he's been covering national security for 20 years. Like, he totally gets that world…spies and secure comms and all of that. So…it really came from him saying, you know, 'I think this is not just going to be affecting national security reporters. I think it's going to be affecting all of the political reporters and nearly all of the journalists in our umbrella.' So we started small by…piloting with a few people, but…ultimately rolled it out to the whole newsroom." (Interview, P29, December 4, 2019, p. 1)

Another journalist agreed that top leadership was essential for security to be infused throughout a newsroom. He said, "It's got to be from the top down, it's got to be leadership. It can be suggested and brought on by reporter-level people who take this seriously and are experts. I think that's a good thing, but they need to be making their pitches as high as they can, because inevitably the way the capitalist structure of a newsroom works is management can force things in a way that the average reporter in the investigative unit cannot." (Interview, P10, June 17, 2019, p. 11)

Another local journalist agreed, and described how, in her organization, security awareness started with her managing editor replacing their morning

meeting on Wednesdays with training sessions that covered a variety of new tools and techniques, including security sessions, that were peer-led. (Interview, P13, June 25, 2019, p. 5)

Some interviewees suggested that the more technologically inclined and young a news organization is, the more nimble and savvier they might be about security. According to a cybersecurity reporter, "BuzzFeed has a great security culture. They have a security team that is a whole-of-company team. It's basically two guys. Very involved in the newsroom, very forward-thinking, very creative. There's whole kits for when someone's gonna be traveling abroad, especially to a country…where evil maids might be a threat. Probably goes overboard, but it's one of those 'better safe than sorry' things." (Interview, P4, April 3, 2019, p. 3)

Others have described how smaller newsrooms that were "basically born of paranoia and of thinking about mass surveillance" like *The Intercept* have a "digital security training mindset" and an "operational security mindset that's just ingrained into the way they do everything" although "not always perfectly." (Interview, P18, October 16, 2019) Others described how *The Intercept*'s "governance structure" facilitates security even on a small budget. An information security technologist said, "…they've shown that you can be small and not have a big budget and be scrappy as long as you have a security team…[and the] team has

power to slow things down and force people to do things and work on stories. And you can get stories you can't normally get." (Interview, P28, December 4, 2019)

A media lawyer for an elite news organization said he thinks security implementation is "scaled appropriately to what reporters are doing. I think our reporters who were engaged in national security work are much more attuned to the need to use Signal or WhatsApp or meet in person…I think that risk prevention should be scaled to the reasonable risk perceived. And if you're covering the New York City school system, you probably don't need to think about those things in the same way that if you're covering the NSA. I think most reporters who are doing anything that sensitive, you know, it needs a higher level of confidentiality, are much more aware of the digital tools available. So you see people saying, you know, 'Can I call you on Signal? Can I call you on WhatsApp?' where before they would just call." (Interview, P3, March 29, 2019, p. 5)

Even in newsrooms that have security awareness at the top level, cross-collaboration related to security issues is needed to provide a more holistic response. "At *The Times*, there's the information security team, there's a corporate security team, there's an international physical security team, there's legal. You have a separate networking team, and you also have a separate team that is the IT Help Desk and the team issuing your laptop…and there's some engineers in the

newsroom, as well," said Sandvik (Interview, P23, November 11, 2019). To address the intersecting challenges that arise, *The Times* uses working groups with various stakeholders for a more thorough and comprehensive evaluation of a threat from all angles (Interview, P15, July 5, 2019, p. 10). The coordination depends on the issue at hand and can involve the information security team and legal.

It's also important for reporters to get to know the information security team so they can reach out to them when they have a question and so that the security team can better understand the unique pressures and challenges facing journalists and how to best integrate security practices into journalists' existing workflows. The development of these relationships helps to build trust. Said Sandvik, "…it is one thing to share your potential story with general counsel of the company and a bit different to share it with the security person who joined a month ago…It takes time to get to know people and build that level of trust just for them to know the different things that you can help with…" (Interview, P23, November 11, 2019, p. 10)

It is also important to assess the different needs of a news organization, whether it's the business side or editorial and adjust training materials accordingly. "For the newsroom, this has shifted to more, "how do I protect my social media accounts, and what do I do when I'm getting threats and harassment online?' 'How

can I reduce that footprint online and how can I securely communicate with my sources?'" (Interview, P12, June 25, 2019, p. 1) She said it's not just recommending a certain technology or app to use, but articulating the reasons behind the recommendation so journalists can dynamically pivot to a different tool that works better for their sources.

Security needs to fit the needs and culture of the newsroom while also addressing the business side of the news organization.

> I think for journalists, it's more personal when you're talking about security, whereas [on] the business side, we're talking about maybe how to protect the company's data, and how do you securely manage it and make sure that only people that need access are accessing it, and with the newsroom, I feel like it's more important because there is this gray line between your personal life and your professional life…I think the need for it is higher, for the newsroom, just because it crosses more over in a personal life, but actually getting them to sit down and dedicate the time to devote to that is where the challenge lies. I think part of that is how do you actually get somebody to sit down and talk with you about it is you really have to be clear, to communicate the value of what you're trying to do with that person in order

to get their time and dedication to that thing." (Interview, P12, June 25, 2019, p. 2)

In smaller investigative outlets, a newsroom might form a team of reporters, their editor, a security person, and a lawyer to talk through a threat model and help figure out what it is safe to talk to the source about, and how it might be safe to reach out to other people and give them certain information about the story. (Interview, P20, November 5, 2019, p. 18) Such collaborations are often decided on a case-by-case basis in his newsroom and aim to integrate security into the journalist's workflow and provide resources for the reporter to ask security questions. (Interview, P20, November 5, 2019, p. 18)

Some security knowledge is shared during onboarding, but security needs arise outside of that time/scope, and need to be addressed as well. And, of course, training sessions need to be interesting to ensure journalists attend and retain the information. According to one digital security trainer, "…we've tried to determine the things we offer in a quarterly by either demands…and based off of where we see the need…we'll create a training that we can offer on a regular basis to ensure that everybody understands what this looks like and how they can protect themselves against it…Obviously, when someone joins the company, we have a set of information that we want all employees to be on the same page with, and we at

least get one time to talk to all of our employees about that information, but there are things outside of that that just are going to continue to be an issue and something we definitely have to remind people of…Obviously, passwords are always going to be an issue, but I will never offer a quarterly training on how to have a secure password just because it would be impossible to get people into that training." (Interview, P12, June 25, 2019, p. 6) Instead she said she integrates those important pieces into other training sessions.

In organizations that have information security teams, these teams may use flashpoints such as current stories about security to raise newsroom awareness about certain practices. This may take the form of reminders from the infosec team to be extra vigilant or to take specific steps. (Interview, P15, July 5, 2019, p. 23) Digital security trainers may try to build buy-in collectively across the news organization by talking about the effect that insecure practices can have on the organization. One phishing email sent to HR or to the style desk can "impact the integrity of the organization as a whole." She added that "when Trump calls *The New York Times* the enemy of the people, we can use some of that messaging to help us further emphasize the impact of different security missteps across the organization." (Interview, P12, June 25, 2019, p. 8-9)

According to a digital security trainer, the development of an information security culture within a newsroom is "actually a very, very new phenomenon." (Interview, P18, October 16, 2019, p. 3) Another, at an elite news organization, agreed. She said, "I've been in this role for a little over a year and I'm the first person [in a role] that's really dedicated to the specific training…We've obviously had an information security team for multiple years and we've even had people who were more dedicated to information security in the newsroom, but training has never been a specific part of someone's job. This is a new approach and I'm trying to figure out the best way to work with people and get people's attention, what type of training really is most impactful, and it's totally different from the newsroom side to the business side." (Interview, P12, June 25, 2019, p. 1)

Although many large news organizations have long had IT teams that have worked to ensure various aspects of network security, there has been a subtle shift in some contexts. "Runa Sandvik's work at *The New York Times* is a testament of how that is being done right now, and is in many ways leading the way on that." (Interview, P18, October 16, 2019, p. 3) The relatively recent departure of Sandvik from *The New York Times* sent shock waves among many in the digital security community. Said one information security technologist, "…people thought oh wow, *The New York Times* is taking some new steps but she's [Runa's] not there

anymore…and there wasn't enough time for that to become a thing that other newsrooms followed." (Interview, P28, December 4, 2019, p. 16) He said that he used to think growing the security culture of a news organization was about getting individuals for a specific role related to information security. Now, he's not so sure. "I used to think it had to do with getting that person, but seeing the way that it turned out with Runa, I'm like 'well maybe it needs to be something that lives in all the reporters.' And it starts with J School…" (Interview, P28, December 4, 2019, p. 17). Yet, many journalism schools are not teaching journalists about information security, indicating that information security techniques and knowledge-sharing also needs to be addressed in news organizations.[34]

The emergence of the young and technologically savvy reporter

Information security in journalism is evolving slowly. Newer reporters and some IT people are skilled in information security, but that's still somewhat rare. Cultural change comes from new hires who are younger and more technologically inclined than some of the more established or older reporters and managers in the newsroom. Said one information security technologist:

> I think there are digital deputies. There's technologists…there's these people who are seen as younger and more techie. And there's an idea that they know

[34] https://freedom.press/news/why-arent-more-journalism-schools-teaching-security-hygiene/

> what the security tools are. And that's what's probably leading the way more than anything else…The younger reporters who've been doing this as part of their career, you know, they bring it in. (Interview, P28, December 4, 2019, p. 16)

This same technologist said, "Young journalists almost think too much of the source technology thing. Like they all learn that you're going to meet one person. They're going to, you're not going to know who they are. They're going to give you like 10 terabytes of data that's going to get you a Pulitzer or something like that. That's not true but, you know, that's what they all figured out…but because of that they're really into information security." (Interview, P28, December 4, 2019). He is hopeful that security cultures will emerge with the younger generation because eventually they will become reporters and editors and will influence the business of the paper. He said, "But until then I think the hope is with the reporters. And the hope is with the reporter learning more about this stuff like becoming the kind of Bart Gellman person" who came in with little information security knowledge but ramped up because he realized it would help with a story and then it paid off with a Pulitzer. (Interview, P28, December 4, 2019)

"…Eventually…more and more editors will be younger and more technical," he said. "And then they all actually teach their teams with stuff…it's an

issue that will take care of itself if we do nothing just because people will age out, right?" (Interview, P28, December 4, 2019, p. 17)

Another information security technologist agreed, and said that security culture will emerge as younger tech-savvy journalists rise in the ranks at newsrooms around the country.

> …what that needs to look like is us all kind of holding each other to better account for making sure that we are protecting one another as well as our sources. I think that right now it's a lot harder to change that culture within a newsroom because they have such established cultures. And often top down leadership but doesn't necessarily always buy into security as something that they do need to prioritize in order to get the work done. And I think what we're seeing is a younger generation of journalists who spend most of their time getting their work done, or playing, or learning through computing. And so it's something that is part of your practice. It's part of how you get everything done. And so it becomes a sort of necessity to learn it even though it's not necessarily something that you care about on the face of it. It's just something that is in the background. It's part of your life. It's part of the culture around you. And I think that it will be easier over time to build that kind of culture within newsrooms, but right now we're kind of in this

intermediate place where, yeah, we definitely have to be very deliberate about building that culture. It's not something that we could just take for granted in newsrooms. (Interview, P25, November 20, 2019, p. 16)

4. Lack of Security Cultures

The development of a security culture in a newsroom is affected by the financial distress and labor precarity affecting many newsrooms. “I mean, there are some newsrooms who don’t think that they need a copy editor or who don’t think that they need other very crucial roles…I think there’s just some barebones decision-making happening and it’s like, ‘Who are we going to eat first?’ (Interview, P29, December 4, 2019, p. 8) As such, information security may not be as prioritized. “I suspect that because we’re so busy, because 2020 is coming, because everyone’s newsroom got cut last year, because of so many pressures and reasons” a step back to look at security needs across the newsroom isn’t happening. (Interview, P29, December 4, 2019, p. 12) Another journalist said that within the local news room “there are so many other things that take priority. Like, if the business model isn't working, then security isn't really a concern…You need to be able to pay people.” (Interview, P16, July 12, 2019, p. 14)

Institutional change can be slow because security might not be a priority and resources may not be available to reporters. A digital security trainer said that he tends to cater workshops to what journalists can do as individuals, in part because institutional change can take a long time. “We want to give them something that

they can take home with them right away." (Interview, P18, October 16, 2019, p. 9)

The journalism industry has been "very guilty of throwing new technology at journalists and then not supporting them into creating good habits around them," said one interviewee. She recounted how when journalists were learning how to use email, "everyone had to go to these like terrible two-hour 'How to Use Outlook' training sessions and then…never got training on how to use email again…or we demanded that every reporter get on Twitter, and maybe they went to a brown bag lunch…or maybe they got to sit down one-on-one for thirty minutes with a social media editor, but…we forced them into this space for Twitter and Facebook and said, 'Here, now you work here,' and kind of never really continued that conversation, and I think that same thing is happening now with digital tools and information security…we're putting people in charge of a lot of information, whether it's the CMS or they're managing edits in Google Docs or they're using Dropbox to manage files or whatever, but we're using these third-parties, we're cobbling things together, and we really need to be cognizant of the risk." (Interview, P29, December 4, 2019, p. 12-13)

Reluctant editors and management

Tensions between editors and journalists can limit the development of security cultures because of differing motivations and temporal demands. Journalism is sometimes viewed as an individual and competitive sport because journalists may be trying to position themselves to get the stories they want to cover. There is sometimes concern on the part of the journalist that if a story is taking them too long because they are trying to use secure methods, they could get pulled off of it by their editor. According to one information security technologist and former data journalist, this can be "a strong motivation for what I would call sloppiness. But you know, understandably being sympathetic, that's just what it is." He suggested having an editor attend a session on how "a really juicy story" was made using security tools to get the editor excited. "Then they'll be like, oh cool, we could do that. I want that story for my team." (Interview, P28, December 4, 2019, p. 5)

Tensions and insecurity may arise as a result of journalists wanting to use secure methods with their sources, but their editors might not know about those methods or why the journalist thinks they are important. "So you have to explain it to your editor. Like, 'Oh, I didn't get to talk to them [the source] yet because they're still installing the app.' They're like, 'What app? What are you doing?…you

need to have buy-in and trust from your editor" (Interview, P28, December 4, 2019, p. 4) because if they don't understand why you are using something, the temporal demand for getting the story might outweigh using more secure methods to develop it.

Alternatively, sometimes editors will look to the reporter. According to one national security reporter, "I think there's a certain reverence that comes with [the cybersecurity beat]. I've usually had the approach that if you tell an editor or someone higher up the masthead, 'We should be talking this way, it's just kind of standard security practice and it's easy,' they'll say, 'Oh, that's standard security practice, okay, then I'll at least have that as an option.'" (Interview, P4, April 3, 2019, p. 3)

Individuals within the newsroom talking about security are not necessarily in a position of power to change the technologies that individuals use throughout the newsroom because they do not hold the purse strings. (Interview, P10, June 17, 2019, p. 8) If "you're just a reporter that's really into security and you want to make it so everybody does things better" then you need "buy-in from the people at the top." (Interview, P20, November 5, 2019, p. 8)

But top management is not necessarily focused on technology or security. "I'm trying to think of a major general news organization that's put a

digitally-focused person at the top. It's hard to think of," said one journalist. (Interview, P10, June 17, 2019, p. 8) Another reporter remarked that "management has a lot to think about, and it's not necessarily in the day-to-day work, and thinking about how the tech comes together. They're thinking about higher level things. It's hard to find a balance between what they're thinking about, and what we're thinking about, and how those things combined." (Interview, P14, July 2, 2019, p. 10).

Other times, management may encourage physical security awareness and training, such as through active shooter drills following the attack against the Annapolis Capital Gazette, but this does not translate to other dimensions of security like information security, which according to a local journalist is "not a common conversation" at her organization (Interview, P16, July 12, 2019, p. 1) She said she would like to see "practical solutions" for improving physical safety and she thinks digital security should be compulsory or otherwise enforced by certain policies so it's not up to the individual reporter to be secure. (Interview, P16, July 12, 2019, p. 6)

Others cited age and an establishment orientation for the reasons behind the reluctance among managers and news organizations to shift their thinking. Said one information security technologist, "The higher up you go, the more...cis white

male above 40-something, maybe 50-something years old you go" and "you'll hear people argue that it's safer to go back to old school methods, like 'Isn't it better if we just gumshoe it and just pound the payment?' and it's like no, actually, that not how it works." (Interview, P28, December 4, 2019, p. 8). Another journalist said that in her newsroom, "…most people have been open to learning newer things in general, but specifically for security stuff, like I said, it's not a usual culture. It's not something that we are told to keep in mind when we are pursuing sensitive stories. So, if they're not told what's out there or what they should be doing, because they've not grown up with technology" then older journalists may not be adopting certain secure technologies. (Interview, P16, July 12, 2019, p. 3)

Even in news organizations that do spend resources on information security, journalists indicate that they would like more resources to be available to the journalism community. "I wish that we had more resources for information security and communication security in journalism in general…I don't think publications still understand how much this is important and how much this is worth investing in." (Interview, P19, October 29, 2019, p.6) According to a digital security trainer, "we're in this moment where newsrooms are playing catch-up a little bit and trying to figure out, 'Oh, okay, it turns out we do need to train people on digital security. We do need to have serious conversations about what happens

every time we publish a politically sensitive article and we know it's going to piss off a lot of readers and we're going to get negative comments. We might even get threats to our journalists.'" (Interview, P25, November 20, 2019)

But he said he hasn't really seen well-articulated ideas about how newsrooms could implement policies or to what extent there is collective buy in on the policies or enforcement mechanisms behind policies. Many newsrooms "don't have any obvious game plan" for this and could invest in resources so journalists don't have to handle all the negative consequences they are likely to face for reporting on stories of import. He suggested that newsrooms could consider budgeting in anticipation of threats that will hit the newsroom, such as organized harassment against journalists writing about certain issues. (Interview, P25, November 20, 2019, p. 7).

Journalists called on those in leadership positions, whether they are chief technology officers or editors, to get on top of security challenges and work collectively. One journalist said that they "should be assessing the situation and saying, 'Hmm, security seems like a big deal right now. Who is handling this in my organization?' and hopefully, those two people will come together and come up with a plan together, but again…that's a big leap of faith that two high-ranking leaders would think to seek the other out and create like a strategy…at some level,

where does the buck stop on making sure your newsroom is happy, healthy, functioning and working?…is that the responsibility of the editor in chief, managing editor, the executive editor, the publisher? I think whoever is held accountable for that really needs to be asking these questions right now." (Interview, P29, December 4, 2019, p. 12)

A security technologist remarked that news organizations are slow to change in part because it's "a very old industry" with "old money." "They think the old, basic ways…they run an old way, but that's what's kept them going" (Interview, P28, December 4, 2019, p. 8). He continued, "…if the business is run using old methods, institutional methods of old school journalism, well then you've got an uphill battle and it's going to take a long time, but it's worth it…and you should understand that it's worth it. Three years is not a long time in this industry." (Interview, P28, December 4, 2019, p. 8)

Another journalist said that management disarray limits security cultures from developing, which can result in reporters receiving online harassment without effective mechanisms to mitigate it. "Sometimes I don't even know when my story is going to go up," she said. "Our team currently doesn't have an editor…by the time I know that my story has been published, there are already comments…I get message requests because they can't reach my main inbox…My Facebook is

heavily locked down, but still…I keep [Twitter] open. Because I've gotten good leads as well from there. I feel like, as a journalist, you should have some means of communication open." (Interview, P16, July 12, 2019, p. 13) She said when she brought up her concerns about being harassed online to her editors they were like, 'Yeah, we are trying to figure this out.' So, I don't know what can be done..." (Interview, P16, July 12, 2019, p. 5) She called on management to offer training sessions related to security because training "should be as important as getting the right facts." She said "we think a lot about protecting our sources, but we don't think so much about how we are protecting sources. Like, not revealing their name is just one very little part of protecting our source. There are many other ways that can be revealing…And for someone to know these things, you need to have trainings…even if you don't have the capacity to get people from the outside, there are enough of us in the newsroom who care enough about security to do these trainings. So just try to tell people to install some apps and use them. Making it a habit instead of, 'Oh, this is something only a few tech savvy young reporters know.'" (Interview, P16, July 12, 2019, p. 4)

There is also a need for security to be scalable for the whole newsroom. According to a cybersecurity reporter "…Ideally, what you want is [to] have a good staff of people that understand information security…My knowledge comes

from just learning myself about it. But that's not something that scales very well. You need to teach your reporters, editors about this. And ideally, you need to have a staff of actual information security engineers and analysts or whatever you want to call them, that are, every day, paid to protect your newsroom and not just with products." (Interview, P19, October 29, 2019, p. 7)

Over the last several years, more organizations have adopted SecureDrop, indicating that awareness about security is on the rise. "SecureDrop is relatively expensive," says a cybersecurity journalist It is an investment that you have to make, but it is another tool that probably media executives feel like, 'Okay, we paid for it. It's there now. We don't have to worry about it.' It's almost a one-time investment, right? I mean, it does require some maintenance, but it's basically like, I don't know, installing a ramp at the entrance of your newsroom. Once it's there, it's there and you don't have to spend too much money on it." (Interview, P19, October 29, 2019, p. 7)

Interdepartmental conflicts with IT and management concerns

Despite these nascent security cultures, there are still tensions and frictions between different departments within an organization as well as between journalists and IT. One media lawyer said trying to have the Chief Information Officer get everybody on the same page with information security practices is

"let's just say, that's a bureaucratic hurdle." She shared how her organization utilizes two-factor authentication "on a lot of our stuff because we're forced to. I certainly wouldn't do it on my own initiative, but they make me do it. That's fine. They can only do so much before people start pushing back." (Interview, P2, March 27, 2019, p. 8)

Sometimes IT teams may block Virtual Private Networks or Tor within a newsroom even though the reporters there are being advised by outside security experts to use those technologies. (Interview, P18, October 16, 2019, p. 3) This can lead to a situation where there are the official applications and tools that journalists are allowed to use, but to implement security tools necessary for their work, journalists "go rogue." Such an environment leads to what security experts have called a "shadow IT culture" where you have reporters "going rogue on their own" with their own tech setups and their own lines of communication that are outside of the domain of their IT department." (Interview, P18, October 16, 2019) According to a media lawyer, people who run IT departments come from different backgrounds, including management, and are really good at figuring out what is needed within a certain budget, but this doesn't always result in cutting edge and creative ways of dealing with problems (Interview, P2, March 27, 2019, p. 13). Sometimes a news organization has IT staff, which has "really smart policies" in

place while other times the "policies are impediments to getting work done…but they're also important policies and the newsroom just needs to get better at communicating the rationale to staff…" (Interview, P2, March 27, 2019, p. 4)

Information security in a news organization is broader than the newsroom

News organizations thinking about how to grapple with information security also have to look at the media organization as a whole business. The separation of business and editorial can complicate the security picture and require solutions for both parts of the organization, which are different despite being "joined at the hip." (Interview, P17, July 12, 2019, p. 13). This becomes a "balancing act" says Sandvik. It can be difficult to justify having a dedicated person in the newsroom. As a result, people are trying to engage more with newsrooms in different ways and are trying a variety of approaches, initiatives and programs. (Interview, P23, November 11, 2019, p. 12).

A lack of bureaucracy more likely in smaller organizations does not necessarily mean robust security awareness or security process. "Here in the Acela Corridor, everybody kinds of knows each other, pretty chummy...people in DC and New York know how to use Signal…it's not a thing that is new to them. Whereas…outside of this bubble…you run into the real world where most people

don’t actually use Signal or know why the cops can read Facebook messages.” (Interview, P18, October 16, 2019, p. 7)

And small organizations may rely more on freelancers. Said one digital security trainer about journalists working in a small news organization or as freelancers: “If you're in a small media org…you're in a wework for example and there is no IT team and you're just kind of like downloading whatever you want on your own laptop and kind of doing things on your own that way. Then there's like less roadblocks but then you know, you don't have a team of people to guide you on like how to use all of these things necessarily… it's kind of like a weird opposite of…not having a digital security team that you can go to for help but then also there's not an IT security team that is like blocking you from doing things and like downloading the apps that you need or whatever.” (Interview, P18, October 16, 2019, p. 4)

Tensions between journalism practice and security

Visibility versus secrecy

Journalists have to be visible online for their jobs, but this visibility comes with risks and companies do not always provide resources or protections necessary to protect journalists. Said one cybersecurity reporter, “being very open, it’s

definitely a double-edged sword…we have a tips page with all our phone numbers and the link to our SecureDrop and stuff like that. And that's great. But it's also like yeah, maybe someone will take that phone number and try to figure out where we live or even just try to hack us." (Interview, P19, October 29, 2019, p. 6)

An information security trainer said that because "journalists are such radically public facing people" there are online mobs or people who are interested in not only attacking the quality of a journalists' work, but also the credibility of the individual and the newsroom and trying to discourage other people from covering similar issues or going into journalism. He said, "I think that newsrooms now are in a place where they need to recognize that it's a serious problem, that people don't want to do this kind of work. You could probably get paid to do a similar job somewhere else where you don't have to deal with all of this potential trauma." (Interview, P25, November 20, 2019, p. 8) Yet, journalists indicated that many publications still don't understand how important security is for journalists or how much it is worth investing in. One journalist said, "I don't know why they don't invest more, but I think that my guess is that they probably don't see the return. And also it's so hard to measure the return of that investment, right?" (Interview, P19, October 29, 2019, p. 6)

Verification versus anonymity

More news organizations are adopting SecureDrop, which requires some maintenance but in many ways is almost like a one-time investment in providing an avenue for more secure communications. Yet, even SecureDrop has had its challenges. Previous research on SecureDrop has indicated that those who have used it have found the system to be generally valuable as a reporting tool, if not particularly consistent. Having SecureDrop has also served as a signal that their organization takes the protection of sources seriously.[35] One interviewee indicated that it has provided decent information but might not have served as much of an enticement as some reporters and editors had hoped. Additionally, she noted that it can be challenging to verify information that is received via SecureDrop, which can make reporting a story harder. (Interview, P2, March 27, 2019, p. 5)

Usability versus security

Some people in newsrooms are technology averse, and it is hard to teach them new technologies, said one data journalist. "If we can make stuff a little more usable, then it's easier and easier to make the pitch." (Interview, P10, June 17, 2019, p. 9) Another journalist and digital security trainer agreed, "I've never had anybody be like, 'I'm going to die on the hill of not signing up for two-factor

[35] https://www.cjr.org/tow_center_reports/guide_to_securedrop.php

authentication,' for example, but I've definitely had people say, "This is cumbersome, this is fiddly; I don't like this," but at the end of the day…this is what it is to do journalism in tech—in an online world. It's time to put the typewriters down and fire up the VPN and get out there and do your job." (Interview, P29, December 4, 2019, p. 13)

Comfort versus security

There is a lack of information literacy among members of the newsroom leading to insecure practices. Said one local journalist, "Slack is a huge problem. We don't have a paid plan, and we have enough channels where stuff vanishes after three or four days, but even then, they are archived. They don't vanish into thin air. So, if someone decides to pay, all of those things would come back. And also, anyone can take screenshots. Screenshots are a problem no matter what you use, except for Snapchat." (Interview, P16, July 12, 2019, p. 8)

Immediacy versus security

Journalists are often focused on the here and now, but a security mindset is longer term and more ingrained into one's habits. According to a digital security trainer, "…there's like something in their ether…it's like we have to tackle this story, *today*. Even though…it will still be a story tomorrow, but no, *today*." Their attention to what people would be willing to read is a type of "sixth sense" but

"developing digital security sensibility is a different kind of sense where it needs to be something that becomes a mindset" with inbuilt practices that become a habit. He said that takes a lot of proactive learning, and normalizing some of these tools in journalists' day-to-day. "It does take developing a threat model in your mindset, an operational security mindset." (Interview, P25, November 20, 2019, p. 14)

Journalists and their sources

Journalists also need to balance using security tools with not scaring their sources away. Said one information security technologist and former journalist, "…You have to walk this line between having them use something that's maybe digitally safe or encrypted or whatever, without scaring them off, freaking them out." (Interview, P28, December 4, 2019, p. 4) Another journalist indicated that there is a misconception among reporters that sources know what's safe to use. "…I think it's really naive and a little honestly self-serving that reporters say like, oh, the source wouldn't be doing it" if it wasn't safe. It's a "frail concept of informed consent…very often the sources don't really know what kind of risks they're putting themselves [in]." (Interview, P24, November 19, 2019, p. 4)

Lack of metrics and knowledge sharing

Interviewees acknowledged that information security practices and policies are not standardized within or across news organizations. According to one journalist, "There doesn't appear to be a gold standard. There doesn't appear to be like a—"Hmm, what do we call this person, what should we pay this person? What kind of experience should this person have?" I don't think we've reached that kind of consensus yet. It feels like the early days of social media, like 2009, 2010…It's hard to make the case for a non-content creating position, even though it's a very important position to have." (Interview, P29, December 4, 2019, p. 8)

Additionally, there are significant challenges with figuring out the efficacy of strategies for advancing newsroom security. (Interview, P25, November 20, 2019, p. 5) Part of this stems from a lack of formal knowledge sharing. Unlike in other sectors such as banking and retail, information security is a newer space for news media and there are much fewer, if any, formal channels that exist where journalists and information security technologists can share concerns and responses to information security challenges in the newsroom. Instead, according to one information security analyst for an elite national news organization, there tends to be a reliance on personal connections and contacts more than established processes like an Information Sharing and Analysis Center (ISAC), which exists in other

spaces like finance and commerce. (Interview, P15, July 5, 2019) To begin to address this, a year and a half ago, Sandvik started a knowledge-sharing initiative for security teams to get together and chat and figure out how to approach certain problems and talk about what's worked and what hasn't. Sandvik says the initiative is still going although it is not active right now. (Interview, P23, November 11, 2019)

Another digital security trainer said that she and her team are trying to "open source" information about security for journalists. She said, " I haven't seen a whole lot of organizations sharing information around, which is why we felt the need to bring it to IRE and NICAR…We also want to more easily open source this information so it is a little bit more accessible." (Interview, P12, June 25, 2019, p. 16)

For the small number of news organizations that do have a formal information security team, the individuals who comprise those teams are still trying to ascertain what types of new challenges reporters face. According to one information security analyst who works for an elite news organization, the security team needs to provide flexible and bespoke solutions that fit in with journalists' workflows. Security teams can't just block a website or strictly limit access like they might do if they worked in a different kind of organization. "The security

landscape is very different in the media…we don't want to just say 'Oh, that's a bad website. We'll block that'…or create hard and fast rules, because oftentimes reporters, depending on what they are working on, need access to different things..."(Interview, P15, July 5, 2019, p. 1).

Additionally, members of information security teams within newsrooms have indicated that they need a better way of measuring the success of their efforts. Currently there are few metrics to evaluate how journalists are improving their information security practices. One director of information security for an investigative newsroom said that he is developing a tool to better assess what journalists are implementing, and what is not working for them in the newsroom. The tool is still in testing, but he is hopeful it will be helpful in improving and ensuring that information security practices are more of a habit. Even in his news organization, with two days of "super intense" onboarding where they learn "just tons of stuff," there is a concern that once journalists get into their work, they resume their normal habits and they don't always bring in the security team when a story is sensitive (Interview, P20, November 5, 2019, p. 9 and 19). Another challenge is that some technologists are not privy to how journalists do their jobs and the different motivations they and their editors may have in newsgathering. According to one information security technologist, "most technologists have no

visibility to any of this. They don't understand how the sausage is made and therefore…it's an extra challenge when you're trying to do this kind of training work or whatever with a reporter. You don't understand what reporting is." (Interview, P28, December 4, 2019, p. 5). Additionally, journalists also tend to keep their security tools close to the vest. "People don't want to talk about what it is that they're using to do certain things (Interview, P8, April 19, 2019, p. 2). According to an information security analyst at an elite news organization, getting newsrooms to care about information security is a dynamic space. She said, "At the end of the day, the news has to go out, and we have to find creative ways to embed security into workflows in a way that doesn't pose an obstacle for our journalists to report the news. A lot of that comes with training and education around security practices so it becomes part of day-to-day practices, rather than a burden." (Personal correspondence, P15, April 29, 2020)

Security is reactive

One reason information security practices are not more diffuse is that actions related to security tend to occur after an incident. According to an information security technologist who works with journalists in newsrooms, the pattern he has seen is that something bad has happened and then management gets together to address how to prevent that bad thing from happening again. It's rarely proactive in

nature. (Interview, P18, October 16, 2019, p. 5) “People don’t really think that they’re going to be the target of online harassment until it happens” or they don’t care about security “until they are hacked.” (Interview, P18, October 16, 2019, p. 10) An information security trainer for a large, elite news organization said information security requests from journalists are rarely proactive. She said, “usually…it’s very reactive. Something happened and they need help.” (Interview, P12, June 25, 2019, p. 3). As another information security director put it, “I think that being proactive requires a whole lot of work and a whole lot of being on top of everything. I think that unless you are specifically into digital security, then you’re just probably not going to do it.” (Interview, P20, November 5, 2019, p. 12)

The reactive nature of security is not only common among journalists, but among editors and management as well. One journalist who has been harassed for more than a year following the publication of an investigative database said that she “did not know at what point to be really scared. And it’s not like anyone could tell me either.” She said she expected management to come up with a plan and have that in place if the harassment crossed a threshold of some sort and should involve the police, “but right now I know that’s not really a thing” unless someone issues a direct violent threat, “but people are not gonna directly say they’re gonna blow your head off.” (Interview, P16, July 12, 2019, p. 9). She said that she thinks

"something really bad needs to happen for people to take it seriously. Which sucks but that's really how I feel…It's just incompetent management really. I feel like my direct supervisor will take me seriously. But for these things to happen, there's money involved." (Interview, P16, July 12, 2019, p. 14)

Security considerations also can be an afterthought in cross-collaborative projects among different teams in the newsroom. According to one data journalist, "I think in the back of our minds, we're thinking about security a lot, and wondering if we're doing enough. I think the hardest thing is that we're not thinking about it at the forefront…When we have a major turn in our team or a major milestone, then we're like, 'Oh, should we consider security at this point? Maybe we should all move to [our internal tool].' Other than that, we're just going about our day-to-day in the way that we know how, because that's how it was originally." (Interview, P14, July 2, 2019, p. 9) Other day-to-day concerns tend to outweigh people's interest and proactive relations with security needs, yet "no one wants a big security meltdown. Waiting till it gets to that point is pretty traumatic and detrimental to the work you're doing." (Interview, P14, July 2, 2019, p. 10)

Security as individual

Security tends to be perceived as an individual problem and not as a collective issue. According to an information security trainer, "we've done a lot of

newsroom trainings where people are not necessarily always plugged into this idea of security being everybody's job." (Interview, P25, November 20, 2019, p. 4) The individual who requested the training might be a security champion within the news organization, and may have had varying levels of success at rallying people around the identification of this need and taking it seriously. The trainer says he tries to convey the message that security is "a team sport" because even though journalists have different beats and differing levels of sensitivity with their sources, everyone in the newsroom has a lot of access to digital and physical assets in the newsroom and thus has a "shared responsibility" to protect those collective assets. He said that although folks understand the logic behind this, not everyone "internalizes that shared responsibility over protecting those collective assets." (Interview, P25, November 20, 2019, p. 4) A media lawyer agreed and said that people who don't think security applies to them and thus don't take it seriously "can actually undermine and compromise information security for everyone else because they're careless. Those are the people that were victims of phishing attacks." (Interview, P2, March 27, 2019, p. 8)

Security vulnerabilities can also arise with broad access to shared platforms, yet emphasizing the shared collectivity of security doesn't seem to work well for behavior change in organizations. According to an Information Security Director,

"I don't think it does really work to articulate that. But it's true, if one person's Google account gets compromised, and we use GSuite, then what GSuite stuff does that person have access to? If someone's Slack gets compromised, what are all of the teams and channels they have? Slack is a terrible problem." (Interview, P20, November 5, 2019, p. 10)

Additionally, individuals who don't think they are at risk because they don't personally report on sensitive stories can also increase vulnerabilities of others in the newsroom through insecure practices. He said that some folks in his organization engaged in poor password management, but they were individuals outside of the newsroom. He said he thinks people think, "Oh, well, I just edit video or something. I don't need to worry about any of this stuff. Even though they are working in the same building as [our news organization's] reporters." People think "they have a much lower threat model because they never look at sensitive documents." (Interview, P20, November 5, 2019, p. 9).

Another journalist said that she has seen individuals assume information security doesn't apply to them. She said, "I also think sometimes, there is like a misunderstanding when we talk about information security…like, 'Oh, that's not me; that's somebody else,' but like, 'No, no, no. Let's—are you in charge of your passwords? Yes, you are.'" She said it is important to democratize security a bit

and remind people that they are “a citizen of this news organization and you're a citizen of this technology information infrastructure, and so therefore, you need to change your password every once in a while, have a strong password, use 2FA…Like these are the community rules because we’re only as safe as the weakest link.” (Interview, P29, December 4, 2019, p. 14)

Another security trainer said that it’s not necessarily that people don’t care so much as they have other things that they care about even more. They might be more preoccupied with some of the reporting that they need to get out today or tomorrow, so they “might cut corners when it comes to managing others’ assets” such as clicking on a link that turns out to be a phishing link because they are in a hurry and perceive information security practices as slowing down their work. (Interview, P25, November 20, 2019, p. 5)

In other instances, journalists don’t necessarily connect their personal practices to their professional needs for security. The boundaries between the personal and the professional are blurry, especially for journalists who might share private aspects of themselves online as part of their online persona (Interview, P12, June 25, 2019, p. 11). According to one digital security trainer, a lot of people think “they don't have that much to hide in terms of their personal life, but it just gives more of a surface area for somebody to target you and attack you and your

family, and I think that's where people aren't thinking as much or maybe they're just starting to look at that." (Interview, P12, June 25, 2019, p. 11). In response to intensifying issues of online harassment and doxing, she says she walks journalists through how their personal information can be used against them or their family and then she leaves it up to them to draw the line between what personally they'd like to share and what professionally they'd like to share. "In some ways I think that people do need to share aspects of their personal life to keep the human piece into their reporting, and that's fine. I tell people, I'm like, 'That's your decision if you choose to make it, just understand how this information can be used against you, and maybe think through scenarios of what would you do if this information was targeted in some way. What measures would you take to mitigate this if it happened, and what could you potentially do that would make it more difficult from this thing [happening]?'" (Interview, P12, June 25, 2019, p. 11) She used the example of journalists sharing personal information such as the names of their children and their general age range, but encouraged them to think how this information might inform other data points that could reveal more sensitive information like where their kids go to school, what their activities are, and their general location. (Interview, P12, June 25, 2019, p. 11)

Insecurity of collaboration

While security may be perceived as individual, insecure practices also arise through collaboration. Many journalists and news organizations use third-party platforms like GoogleDocs even though doing so presents certain risks while ameliorating others. One data journalist recounted how her team heavily relies on Google Docs. “A lot of the things we do are run on Google Docs. Google has all the stuff that we have at this point. That's not secure at all, but…it's almost like newsrooms everywhere are using Google Docs…knowing the risk that at any point, Google could just decide to just do whatever they want with the document that we store there.” She described how they are trying to use Dropbox more when working with other teams like investigative reporters, but she wonders if that is any more secure: “When we do our project, we still have to put it in Google Docs. For this one project, I'm putting the drafts into the project, which was powered by a Google Doc. At that point, does it even make sense to try to be sneaky with what we're saying? It's already in Google Docs. It's already not very secure. Is Dropbox even that much more secure? I'm not sure. I don't know.” (Interview, P14, July 2, 2019, p. 9)

Other times security concerns come up in the onboarding and offboarding process because journalists use their Gmail email address for work and once they

leave the company they still own a lot of the documents the team uses. Said one data journalist, "…every time we need to get into a document, we just need to send a request to transfer ownership" which is "really annoying." (Interview, P14, July 2, 2019)

Other times it's unclear when or how to move a team of journalists to an internal tool rather than keeping information with Google and also how to ensure journalists are using their work email addresses rather than their personal email addresses for communications. (Interview, P14, July 2, 2019, p. 5)

Journalists and news organizations also need to think about access and compartmentalization when assessing security. Secure processes often require documentation and transferability as well as integration. Journalists need usable technology that is also secure and shareable. Changing insecure behavior is hard because you need to change habits. Said one data journalist, "how we share resources is the biggest barrier to entry…in security…Google Docs is just really easy because everybody uses it, and no matter if you're a reporter who has never touched code or a really well-versed developer, you know how to use Google Docs. Where is the compromise? Where can you compromise on usability versus efficiency, and that push and pull?…It's more to understand, it's more to do, and it doesn't mean that that's a bad thing, but it does mean that people just have to be

willing to learn and change how they're doing things. That's the hardest part." (Interview, P14, July 2, 2019, p. 13)

Ignorance about security

Journalists tend to look to their own networks and communities for insight and knowledge into information security, which can be problematic because "a little bit of information sometimes is a dangerous thing" especially if it's ill-informed or wrong. (Interview, P28, December 4, 2019, p.2) In other situations, journalists may do a quick search online about a tool or application, which can then result in bad information. According to an information security trainer, a lot of people "are using one specific outlet" and "surface-level research" which can become problematic if the story gets more sensitive and complicated. Additionally, it's important for journalists to know the reasons behind why the team suggests a particular tool or approach so they can more dynamically assess tools and methods for their own work. (Interview, p12, June 25, 2019, p. 12) Journalists don't always know if their organization has information security people that they can turn to. Said one data journalist, "I'm sure there has to be people who are thinking about security systems and information security, [but] why don't we know more about them? Why don't we work with them more?" (Interview, P14, July 2, 2019, p. 12)

Security by obscurity mental model

Interviewees noted that many people don't think that information security applies to them. Said one media lawyer, "I do think that it has to feel real to people and I don't think it does. I think there are some journalists that are sensitive to it, but it's a small percentage. I think that the vast majority feel like nobody's out to get them. They're not doing anything that's important, that anybody's going to try to steal their stuff. Even the ones that are doing sensitive stuff feel like they're generally protected…Again, unless they see examples of people getting in trouble and getting busted, like really getting into trouble, I don't see that mindset changing." (Interview, P2, March 27, 2019, p. 10)

Another limitation to the adoption of information security tools and practices in the newsroom tends to be a perceived lack of risk or threat. Respondents indicated that high profile examples of threats or risks to journalists can result in journalists and others in the newsroom starting to care, but that this feeling fades as the perceived risk or threat lessened. Said one media lawyer, "I think that every time there's a high profile example, people start to care, but it fades pretty quickly… I think it has to be real for them in order to feel like it's worth going through the hustle using some of these technologies." (Interview, P2, March 27, 2019, p. 10)

One journalist likened security to a "set it and forget it" type thing. "Like you put the batteries in your smoke alarm and you don't think about them again until it starts chirping at you later, and I think security is a really easy thing to overlook, especially if you haven't had a breach. If you haven't been intimately involved in wide-scale harassment of a journalist or doxing or swatting or being hacked…or whatever the case might be, I think people just think the stakes are really low and they're just wrong, or…they're either misinformed or are…underestimating the risks, and then if you're a security person, you sort of end up sounding like this kind of like tinfoil hat, black helicopter person being like, 'The risks are out there, the risks are out there,' but like really, they are, and so you kind of have to balance with people, convincing them that like they should just do—it's like recycling, right. Like they should do it because it's right and it's better for everybody and everybody recycles, but it only works when everybody does it, right, and so like I often like use that analogy with people who are…kind of skeptical, where it's like, 'Look, this may not affect you directly, but you're helping to protect the entire newsroom and like you should really do that.'" (Interview, P29, December 4, 2019, p. 13)

Anxiety related to security has also become normalized and along with it an acceptance of the new reality. "I think when you live in a universe where someone

who has access to your email can suddenly access all of your bank accounts, all of your children's photos, all of your digital life which represents a huge portion of your actual life, there's a lot more concern," says Hickman. "So I don't think there's a specific flashpoint but I think there's an increasing awareness that each of us has a lot to lose. I did see right after Trump's election there was a lot of anxiety about this coming dystopia and I think some of that has waned. I don't see as much anxiety about it, but I think there are these moments where people are suddenly like, 'Oh wait, I should probably pay attention to this.' Then they pay attention for a while and they may or may not continue to pay attention…It's hard to be constantly putting out fires and I think people get used to things and get acclimated, it's no longer shocking." (Interview, P9, April 22, 2019, p. 11)

Another tension underpinning the implementation of information security technology is the perception of it always being slow. "You have a competing interest in getting the story right and getting it fast. Those things don't necessarily always work together because if you go fast, you might make mistakes, but if you get it right, you're going to be slower. I think those information security practices, you want ease of use, but you also want security, and those things can work against each other. Sometimes you're going to compromise on one or the other." (Interview, P2, March 27, 2019, p. 9) Adoption of information security tools can be

hard, lessening actual adoption. “It’s hard. Let’s be honest,” said a media lawyer. That’s the other thing. People will do anything you tell them to if it’s easy. If it’s hard, if it’s complicated, if it’s inconvenient, if it makes them go out of their way, they don’t want to do it.” (Interview, P2, March 27, 2019, p. 8)

Conclusion

This report has shown how a variety of flashpoints from the Snowden disclosures to incidents of source exposure to ongoing breaches and intensifying online harassment and doxing attacks against journalists have raised the profile of information security needs and practices in the newsroom. News organizations have begun to address information security concerns in a patchwork type way with the adoption of the anonymous whistleblowing submission system, SecureDrop and updated "tip lines" which provide encrypted options for sources to communicate with journalists. More well-resourced organizations like *The New York Times* have hired more individuals in the last two years who have a more specific focus on information security in the newsroom, while other organizations have hired individuals for typical roles in the newsroom who may have more information security knowledge than their predecessors. Individuals throughout the newsroom who believe information security practices are important serve as "security champions" and help to create awareness and buy-in from their peers and leadership to invest in informal brown bag sessions and training seminars so that journalists have the opportunity to learn more about information security. These

security advocates arise from across the newsroom and can be journalists, lawyers, IT specialists, or others who believe that security is important and should inform journalistic and newsroom practices.

Journalists continue to use their own networks to obtain information security knowledge and inform their practices, which can sometimes lead to misinformation and also may result in their bypassing existing security resources. Competing priorities among individuals who hold different roles in a news organization can result in a slower orientation to improving information security knowledge and practices while ongoing financial considerations and labor precarity also continue to carry weight and shape decisions among newsroom management.

Ongoing tensions between aspects of journalistic practice, such as quickly getting and publishing a story, can result in a lower prioritization of some security mechanisms. Journalists and management tend to view security in a reactive pose and are more likely to engage in information security practices following a breach or hack. A proactive security posture tends to occur if a journalist is concerned about online harassment or doxing targeting themselves or their families. Security tends to be viewed as something that is individually important rather than a collective issue that can have repercussions for others in the newsroom.

Additionally, journalists are still assessing how to better incorporate security practices during collaborative projects in the newsroom.

Although interviewees expressed hope that younger and more technologically savvy individuals would bring information security practices into the newsroom and thus slowly shift newsroom security cultures, the deteriorating financial and political environment facing journalists, and the myriad risks and threats they receive, suggest that information security knowledge and training should be prioritized by management, editors, and journalists in the near-term. It would be invaluable to ensure that journalists have additional resources available to them so that they can continue to carry out their work in that heightened-risk environment.

Recommendations: What's needed for security cultures

Below are recommendations for news organizations interested in improving information security awareness, with the understanding that specific solutions should be tailored to the resources, ethos, and management structure of the organization.

- **Enhance interest in security by making it personal.** Conversation should shift away from only protecting sources to protecting selves, the organization reputation, etc.
- **Frame security as an issue of maintaining credibility and ensuring trust,** especially since bad actors remain intent on sowing disinformation and attacking journalism.
- **Harness the dual nature of security helpful for implementation/adoption.** Want a journalist to understand how his or her information is used online? Make it about them and how they could be doxed.
- **Build a champion model for information security alongside the advice of robust, expert-led security professionals.** Leverage internal knowledge of

staff members for peer led training sessions, but also include external experts because sometimes an outsider may be more effective

  - Invest in a trainer or team to help journalists integrate information security practices into their work
  - Help reporters understand what to look out for, how to deal with it, and who to contact when something goes wrong
  - Ensure the information security team is visible, open, transparent and collaborative so journalists know who they are and how they can help

- **Make security fit journalism.** Recognize that information security needs to work within journalistic workflows and not the other way around if you want it to stick and be utilized
  - Teach journalists where information flows, how it circulates, and how they can manage their own information and security processes
  - Develop a dynamic understanding among journalists about the security tools and practices they use or should use so that they can better evaluate what works and why
  - Tailor training sessions to the specific audience, using real-world examples of journalists and news organizations to resonate with the

audience and providing resources during and following the training session

- Encourage more dialogue between journalists and the security team (if a newsroom has one) to ensure knowledge transfer is occurring successfully

- **Develop an ongoing security consciousness and a culture of empowerment around security**
  - Integrate information security knowledge transfer in the onboarding process and in collaborative projects across the newsroom
  - Develop tighter policies around, and budgeting for, the development of tools and practices that will help make newsrooms and resources safer
  - Understand the data retention policies in place in the corporate environment, from Gmail to Slack
  - Carry out internal spear-phishing campaigns and closely monitor journalists' usage of security tools and engagement in security processes

- Develop an “ask a manager” network where journalists could send in questions, which are then anonymized and generalized and get answered and published
- Treat security as a collective concern and not just an individual one, in order to develop collective responses in turn
- Look at security holistically, including how it intersects with legal, physical, and psychosocial dimensions
- Potentially use a security auditing framework and evaluation template like SafeTag: A Project of Internews, and peer to peer curricula like The Field Guide to Security Training in the Newsroom or LevelUp’s Trainers’ curriculum
- Find the right contextual balance between security and usability
- Be able to scale up and threat model as appropriate
- Understand that developing an information security culture needs to be ongoing, iterative and proactive
- Take a comprehensive approach to examining what people do, look at who needs what, and how each process might be scalable for an organization as a whole.

- **Need information sharing of threat intelligence and responses/standards among news organizations**
    - Establish or join an alliance allowing for shared threat intelligence and responses
    - Work on sharing threats and responses to attacks in aggregate among media orgs so it can be an information sharing exercise and help improve the security of an organization
    - Create a database of different types of threats affecting journalists so then these can be used as examples for training sessions and to convince folks about information security needs
    - Stay up-to-date on best practices for passwords, online accounts, software updates, and travel and secure communications

- **Adopt tiered levels of information security in newsrooms**
    - Start with a strategic phishing campaign in the newsroom to raise awareness and understanding of how phishing works and how to limit falling victim to it.
    - Host brown bag sessions related to information security with inside and outside experts

- Have travel related sessions and a loaner device system for journalists reporting internationally or in places of conflict, including protests and political rallies within the US
- Create a 24/7 hotline to report threats reporters face, assessment made by professionals about the credibility of the threat and what to do about it (way threats happen, how to report them, what to do if threatened)
- Provide security resources to freelancers, whenever possible
- Implement basic security measures across the newsroom (see below)

More specifically, interviewees suggested that at a minimum, news organizations should consider investing in some or all of the following:

1. Add two-factor authentication on accounts
2. Train the whole news organization on how to spot a phishing email and what to do if they see one
3. Encourage threat modeling and risk assessments
4. Empower security champions and prioritize security knowledge in who is hired.

5. Add an information security technologist for the newsroom or a larger information security team for the news organization
6. Limit password overuse by encouraging the use of password managers
7. Provide resources for journalists to help limit what information is available about them online to reduce the likelihood that a doxing attempt is successful
8. Learn about and using robust virtual private networks (VPNs)
9. Integrate encrypted communications like Signal into daily life and utilizing the disappearing messages function for sources.
10. Empower oneself by staying up to date on security issues by following organizations who write about these issues (e.g. Freedom of the Press Foundation, Committee to Protect Journalists, etc.)

References

Balsmeyer, L. (2020, January 27). Freedom of the Press Foundation releases its *2019 Impact Report*. Freedom of the Press Foundation. https://freedom.press/news/freedom-press-foundation-releases-its-2019-impact-report/

Bell, E., Zuckerman, E., Stray, J., Coronel, S., & Schudson, M. (2013, October 4). Comment to Review Group on Intelligence and Communications Technologies regarding the effects of mass surveillance on the practice of journalism. Retrieved from https://www.dni.gov/files/documents/RG/Effect%20of%20mass%20surveillance%20on%20journalism.pdf

Berret, C. (2016, May 12). *Guide to SecureDrop.* Tow Center for Digital Journalism. https://www.cjr.org/tow_center_reports/guide_to_securedrop.php

Bodyslams, bombs and shoves: Anti-media violence in Trump's America. (2019, February 12). Retrieved from https://www.axios.com/violence-against-media-bombs-shootings-trump-a59584cb-ac2c-4813-bfef-7b3a4233690d.html

Bradshaw, P. (2017). Chilling effect: Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations. *Digital Journalism, 5*(3): 334–352. https://doi.org/10.1080/21670811.2016.1251329

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage Publications.

Committee to Protect Journalists. (2017, August 2). *New website to track press freedom violations in United States* [Press release]. https://cpj.org/2017/08/new-website-to-track-press-freedom-violations-in-u.php

Committee to Protect Journalists. (2018, November 1). Digital safety: Protecting against online harassment. *Safety Notes.* https://cpj.org/2018/11/digital-safety-protecting-against-online-harassmen.php

Deibert, R. (2017, December 6). Evidence that Ethiopia is spying on journalists shows commercial spyware is out of control. *Wired.* https://www.wired.com/story/evidence-that-ethiopia-is-spying-on-journalists-shows-commercial-spyware-is-out-of-control/

Ferrier, M. (2018, September). *Attacks and harassment: The impact on female journalists and their reporting.* International Women's Media Foundation and Troll-Busters. https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf

Fisher, M. (2013, April 23). Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? *The Washington Post.* https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

Goggin, B. (2019, December 10). *7,800 people lost their media jobs in a 2019 landslide.* Business Insider. https://www.businessinsider.com/2019-media-layoffs-job-cuts-at-buzzfeed-huffpost-vice-details-2019-2

Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). *Building digital safety for journalism: A survey of selected issues.* Unesco. https://unesdoc.unesco.org/ark:/48223/pf0000232358

Ingram, M. (2018, December 19). Every 30 seconds, a female journalist or politician is harassed on Twitter. *Columbia Journalism Review.* https://www.cjr.org/the_media_today/female-journalists-harassed-twitter.php

Lindlof, T. R., & Taylor, B. C. (2011). *Qualitative communication research methods* (3rd ed.). Sage Publications.

Marczak, B., Alexander, G., McKune, S., Scott-Railton, J., & Deibert, R. (2017, December 6). Champing at the cyberbit: Ethiopian dissidents targeted with new commercial spyware. The Citizen Lab. https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Marczak, B., Anstis, S., Crete-Nishihata, M., Scott-Railton, J., & Deibert, R. (2020, January 28). Stopping the press: *New York Times* journalist targeted by Saudi-linked Pegasus spyware operator. The Citizen Lab.

https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/

Marimow, A. E. (2013, May 20). Justice Department's scrutiny of *Fox News* reporter James Rosen in leak case draws fire. *The Washington Post.* https://www.washingtonpost.com/local/justice-departments-scrutiny-of-fox-news-reporter-james-rosen-in-leak-case-draws-fire/2013/05/20/c6289eba-c162-11e2-8bd8-2788030e6b44_story.html

McCudden, K. (2020, January 1). Three years of tracking: Our January 2020 newsletter. U.S. Press Freedom Tracker. https://pressfreedomtracker.us/blog/3-years-tracking-our-january-2020-newsletter/

Office of the Representative on Freedom of the Media. (2016). *New challenges to freedom of expression: Countering online abuse of female journalists.* Organization for Security and Co-operation in Europe. https://www.osce.org/fom/220411?download=true

Perlroth, N. (2013, February 1). *Washington Post* joins list of news media hacked by the Chinese. *The New York Times.* https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html

Perlroth, N. (2013, January 30). Hackers in China attacked *The Times* for last 4 months. *The New York Times.* https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

Perlroth, N., & Sanger, D. E. (2016, August 23). *New York Times*'s Moscow bureau was targeted by hackers. *The New York Times.* https://www.nytimes.com/2016/08/24/technology/new-york-timess-moscow-bureau-was-targeted-by-hackers.html

Petersen, A. H. (2018, Winter). The cost of reporting while female. *Columbia Journalism Review.* https://www.cjr.org/special_report/reporting-female-harassment-journalism.php

Peterson, A. (2014, December 18). The Sony Pictures hack, explained. *The Washington Post.*

https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

Reisinger, D. (2014, March 28). *Watch out, journalists: Hackers are after you.* CNET. https://www.cnet.com/news/watch-out-journalists-hackers-are-after-you-google-says/

Reporters Without Borders. *Online harassment of journalists: Attack of the trolls.* Retrieved from https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf

Savage, C., & Kaufman, L. (2013, May 13). Phone records of journalists seized by U.S. *The New York Times.* https://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. (2017, June 19). Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware. The Citizen Lab. https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

Security Without Borders. *Reports on targeted surveillance of civil society.* https://securitywithoutborders.org/resources/targeted-surveillance-reports.html

Shelton, M. (2019, July 8). Why aren't more journalism schools teaching digital security? Freedom of the Press Foundation. https://freedom.press/news/why-arent-more-journalism-schools-teaching-security-hygiene/

Simon, J. (2019, May 13). The real threat to press freedom is prosecuting leakers. *Columbia Journalism Review.* https://www.cjr.org/watchdog/daniel-hale-intercept-leakers.php

Stockler, A. (2019, June 19). Trump supporter charged with assault on *Orlando Sentinel* journalist covering president's 2020 rally. *Newsweek.* https://www.newsweek.com/trump-supporter-arrested-assault-journalist-rally-1444834

Sugars, S. (2019, January 30). From fake news to enemy of the people: An anatomy of Trump's tweets. *CPJ Blog.* https://cpj.org/blog/2019/01/trump-twitter-press-fake-news-enemy-people.php

Timmons, H. (2018, August 1). *Watch: A furious Tampa crowd screams at the press, just as Trump intended.* Quartz. https://qz.com/1345622/video-of-a-trump-rally-crowd-harassing-the-press-in-tampa/

Waldman, P. (2018, October 19). Trump encourages violence against reporters, and his supporters cheer. *The Washington Post.* https://www.washingtonpost.com/blogs/plum-line/wp/2018/10/19/trump-encourages-violence-against-reporters-and-his-supporters-cheer/

Westcott, L. (2019, September 4). 'The threats follow us home': Survey details risks for female journalists in U.S., Canada. *CPJ Blog.* https://cpj.org/blog/2019/09/canada-usa-female-journalist-safety-online-harassment-survey.php

Women's Media Center. *WMC Speech Project.* https://www.womensmediacenter.com/speech-project/research-statistics

Appendix I: Interviewees

Appendix I: Interviewees

Participant						
#	Identifier	Gender	Org. Type	Role	Beat	Date
1	P0	Female	Nonprofit org.	Director of Newsroom Digital Security	N/A	February 18, 2019
2	P1	Male	Large news org.	Journalist	Criminal justice	March 25, 2019
3	P2	Female	Large news org.	Media Lawyer	N/A	March 27, 2019
4	P3	Male	Large, elite national news org.	Media Lawyer	N/A	March 29, 2019
5	P4	Male	Large media org.	Journalist	National security	April 3, 2019
6	P5	Male	Medium investigative news org.	Former Co-founder, CEO, President and Editor-in-Chief	N/A	April 3, 2019
7	P6	Male	Large news org.	Security Professional	N/A	April 9, 2019
8	P7	Male	Medium news org.	Journalist	National security	April 19, 2019
9	P8	Male	Nonprofit org. that connects journalists and technologists	Web developer and journalist, tech lead for nonprofit org.	N/A	April 19, 2019
10	P9	Female	Small nonprofit org.	Director of Product	N/A	April 22, 2019
11	P10	Male	Independent	Developer and journalist	N/A	June 17, 2019
12	P11	Female	Journalism School	Program associate	N/A	June 19, 2019
13	P12	Female	Large, elite national news org.	Infosec Training Manager	N/A	June 25, 2019
14	P13	Female	Regional journalism collaboration	Interactive developer and data reporter	N/A	July 1, 2019
15	P14	Female	Large, elite national news org.	Journalist	Graphics	July 2, 2019

16	P15	Female	Large, elite national news org.	Information security analyst	N/A	July 5, 2019
17	P16	Female	Local news org.	Journalist	Demographics	July 12, 2019
18	P17	Male	Medium, investigative news org.	Developer and journalist	N/A	July 12, 2019
19	P18	Male	Nonprofit org.	Digital security trainer	N/A	October 16, 2019
20	P19	Male	Small online media company	Journalist	Cybersecurity	October 29, 2019
21	P20	Male	Small investigative news org.	Director of Information Security	N/A	November 5, 2019
22	P21	Male	Independent	Security Professional	N/A	November 5, 2019
23	P22	Female	Independent	Journalist	Security, human rights	November 5, 2019
24	P23	Female	Formerly large, elite national news org.	Senior Director of Information Security	N/A	November 11, 2019
25	P24	Male	Small investigative news org.	Journalist	Investigative	November 19, 2019
26	P25	Male	Nonprofit org.	Principal Researcher	Digital security	November 20, 2019
27	P26	Male	Nonprofit org.	Researcher	Press freedom and safety	November 20, 2019
28	P27	Male	Nonprofit org.	Researcher	Press freedom and safety	November 20, 2019
29	P28	Male	Nonprofit org.	Information Security Technologist	N/A	December 4, 2019
30	P29	Female	Independent	Journalist and former editor at various newsrooms	N/A	December 4, 2019

Jennifer R. Henrichsen is a PhD candidate at the Annenberg School for Communication at the University of Pennsylvania. A former Fulbright research scholar, she has been a consultant to UNESCO and is a coauthor or coeditor of three books about journalism.